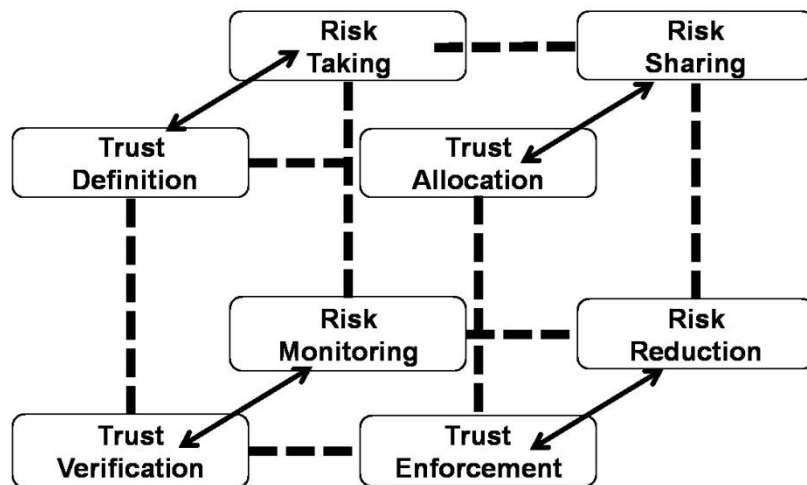


Fundamental Conceptions Of Information As Applied to Identity Logistics

Carlos E. Trigos Sanchez



Published in the United Kingdom – May 15, 2013

Copyright © Carlos Trigoso 2012-2013

Table of Contents

Abstract	6
Preface	7
Acknowledgements	10
Introduction	11
1. Security as a Problem	18
Approach to Security Management	18
The Need to Discuss Security	19
Why does security fail?	20
The Missing Discourse	21
Global Trends in IT and Security Management	23
Theories of Error	25
Enterprise Architecture	27
Wasting Time in an Impossible Mission	29
Information Ideology	30
2. Freeing Security from “Risk Avoidance”	34
A Key Issue	34
Economic Concepts	35
Decision Making	36
How are Decisions Made?	37
Risk and Probability Theory	40
Bayes' Rule	40
Security as Insurance	42
Luhmann on Trust	44
Identity Management Beyond the Standard Approach	45
Trust and Respect	47
3. Security and Information: Access Management	51
Dependency of Information Security	51
Four Classes of Access Control	52
Access and Indirection, Secrecy and Authenticity	55
Modalities of Risk and Trust	57
Information Theories	59
Definitions of Information	60
4. The Context: Identity becomes Data	66
Data-Centric Security	66
What is a Security Policy?	68
Security Assurance	70
Internal and External Actors	73
Secure Identity Management is Data Management	75
Data Quality Criteria in Security Management	77

5.	Identity Services and Programme Delivery	80
	Surveying the Landscape of Failure	80
	The Causes of Failure	84
	IT and Information Security as Business Sub-Systems	87
	Security and Identity Investment Decisions	89
	The Value of IT	91
	Identity Programmes and Projects	93
6.	The Cloud Transforms the Network	96
	Identity in the Cloud	96
	Identity Federations	100
	Cloud Security Concerns and Advantages	102
	Information Technology and Capitalism	104
	Identity Assurance Services	105
	Identity Trends	109
7.	Quantitative Identity Management	111
	Information Value and Flow	111
	Identity and Organisational Transformation	113
	What IT never did, and never will	115
	Enterprise Identity Management Layers	117
	Identity Information Logistics	124
	Identity Data Management is NP complete	134
	Performance Measures	135
	Forms of Identity Management Optimisation	137
8.	When is a System Secure?	141
	Systems and “Systems”	141
	Security “for” and “in” the Organisation	142
	The Paradigm Shift	144
	Dereliction of Duty	145
	Information Insecurity	147
	The current Situation	150
	What Security is not	153
	Outside of the Perimeter	154
9.	Persistence of Techno-Centrism	156
	The Fundamental Conceptions	156
	Empirical Views in Business	159
	IT and Business Conflicts	161
	Four Root Metaphors	163
	System Metaphors	169
	Sociological Paradigms	171
	More than People, Process, Technology	174
	Annex to Chapter 9: The Security Perspectives	177

10.	The Cloud Transition	180
	Security Arguments are Philosophical	180
	Cloud Computing and the Problems of IT	180
	Business continues to evolve	181
	Eclosion of Security Concepts	184
	Risk Focus and the Cloud	187
	Quantitative Identity Management	189
	Facing Reality	191
	After The Clouds	192
	Breaking the Ceiling for Cloud Adoption	194
	Selected Bibliography	198

Abstract

A study of identity information inside and outside the firm, and in exchanges between firms, groups and individuals.

What are information flows and information security? How can we control access to information? How can we measure information in an organisation? How is the return on investment measured in security and identity projects? What are the alternatives to risk-based information security?

Information security principles and practices are applied to propose a model of Security Management Perspectives and their underlying theories of information. On that basis, a new approach to Identity and Security management is developed applying ideas of logistics and performance. The work shows how Cloud Computing needs new ideas of trust and risk management beyond traditional positions.

Copyright © Carlos Trigoso 2012 - 2013

Preface

What we term Completion is enduring achievements that cannot be changed.

Yang Xiong, "The Elemental Changes," 2 B.C. (Translated by M. Nylan, 1994)

I was born in Lima, the capital of Peru, in 1954. My career in Information Technologies started in the late 70s when I applied spatial models to regional development and national economics. I started with Information Technologies as a user, writing programs and using computers, and this gave me a very early look into a trend that ultimately would change not only the world but also my personal career.

I emigrated from Peru in 1984 and continued privately with my work in regional development and economics. I lived and worked in China and Europe until 1999 when I settled in the United Kingdom. While I never abandoned research on history and spatial economics, in practice I moved increasingly deeper into the IT industry. I stopped being only a user and started various lines of business, including software development, network design and installation, computer assembly, systems monitoring and security. I worked for small and large IT consultancy firms including some of the most important in the world, and I also founded and led my own business initiatives in China and Spain.

In all these roles I operated as a technology strategist, an IT architect, a security expert and advisor but without having the benefit of a formal education in Computer Science. I have met many colleagues who also moved from other professions and academic careers into IT, and this makes me think that sometimes a Humanities background is actually an advantage, especially in consultancy services.

After some years in the Finance sector, between 2008 and 2010, I joined a global Consultancy firm based in London in June 2010 and since then I have led professional teams and technology partners in the development and delivery of innovative Security services, mostly related to access control, user identification and authentication. This is reflected in my recent work on Identity Logistics which forms the main area of my experience.

My long career in the IT sector never obscured my personal work in other areas of knowledge. Quite the contrary, I believe that this experience allowed me to crystallise, albeit in a different terrain, the intuitions and ideas that I had formulated in a previous more theoretical period. For years I managed to publish many articles in different countries, in Chinese, Spanish and Peruvian publications, but all of this never achieved a satisfactory level of completeness. The shift to the IT world also didn't help as more and more of my time was absorbed by business activities.

Nevertheless, around 2004, I started to articulate a more integrated view, a more mature grasp of the complexities of the IT world. So, my "second" profession became one with my "first" one. My early

work and orientation to the Humanities converged finally when I sketched the work that has now crystallised in this book.

It is perhaps the link with the past and with other non-technical areas of knowledge that make this book special. This work is not a conventional treatise on Information Technologies, but it is also not a philosophical speculation. I think that I have found the right balance between the transitory and changing world of Information Technology and Security, and the much more permanent values of economic and organisational theory, as well as other classical areas of knowledge. I hope that the reader will see my main contribution and not be distracted by appearances.

My work in Information, Identity Logistics and Security Management is focused on innovation and change from a philosophical point of view. While it is customary to emphasise change and innovation in the world of IT, this is rarely done with a perspective outside of IT itself. Standing on my own experience, I believe that nothing can be achieved by following technological trends while accepting a philosophically impoverished world view.

I see it as my mission to work with my colleagues and clients, fighting against conventional “wisdom” and analysing problems in depth to bring up new approaches and understanding.

I focus my message on integrity and completeness, and my goal is to offer a coherent view and strategy that makes sense for business leaders and all types of organisations. It is my experience that too frequently, world-class organisations get bogged down not by lack of “knowledge,” but by lack of vision, of forward thinking, strong philosophical principles and purpose. This is particularly the case in the Information Security arena, where professionals tend to be “defensive” and “static” with the consequence that they end up resisting change and improvements.

I like to think of my method as “insight-based problem solving.” Starting from my early research in history and regional development economics, where I learned to distinguish between the realities of underdevelopment and the fantasies of economic theory, I developed this approach enriching it with my experiences in many countries as an expert advisor and trouble-shooter. I was able to learn from the fact that –contrary to usual understanding—problems do not arise from technological causes but from the uses of technology, especially from organisational factors.

I developed a systemic solution method to reveal the “organisational blocking factors” which lie at the root of technological failure and financial loss. Coming from a very different context and orientation, it was simple for me to keep my independence and avoid any attachment to particular technologies or brands. This has always given me complete freedom to analyse and see beyond the current technological motives and artificial trends.

Sometimes I classify what I do as “Enterprise Security Architecture,” but probably this is a misnomer. In reality, such a specialty does not exist in the current IT world. IT departments and consultancy houses do understand what “Security Architecture” is, and there are “Technical Architecture” roles in this space, but beyond that there is no concept of a discipline that would bind together the various aspects

of Security. There is no Security Architecture in the same way that there is no Security Theory (as I explain in my book). Even worse is the fact that the Information Security professions do not have any room for philosophy, i.e. for reflection on the fundamentals and presuppositions of our activities. The gravity of the situation can be ascertained when we see that many organisations even have difficulty in seeing Security as part of their Business Model, or their information management strategy, and instead insist on purely technical practices.

In part, my book is a call to IT and Security professionals to look beyond these limitations. This should ideally be linked to some sort of hope in the future, but I confess that it is not clear to me when Security Architecture will become an essential part of corporate strategy. I am very pessimistic about the possibility of this transformation.

Despite this pessimism, my book condenses and articulates the insights and advice that I have developed throughout my professional career, including technical insights but above all a coherent model encompassing Four Perspectives of Security, those of **Direction, Selection, Protection and Verification**. This is my model of “complete action” applied to the Security Arena. I believe that this is a unique approach to Security and this distinguishes my position from conventional approaches in these professions, and I expect that the reader sees beyond this application and into the more fundamental principles.

Another way to look at my work is to appreciate its strong emphasis on methodology. This stems from the understanding that all decision errors are based in wrong methods, while simultaneously it is true that no method can by itself guarantee a good decision. A well-founded method is one that is complete, both analytically and synthetically, one that balances theory and practice, and, essentially, one that articulates the Four Perspectives.

Very often people define an “error” as any decision that leads to loss or failure, but in the complex disciplines of Security –and similarly in politics, economics and the “soft” sciences –good decisions and strategy can lead to negative results, while poor decisions may lead to economic benefits and “success.” This paradox appears when we judge decisions and outcomes only quantitatively, ignoring their complexity, their systemic aspect and the interaction and the long-term consequences. The Four Perspectives allow us to see every decision in a much wider context.

We must learn to see when immediate “success” becomes worthless, when opportunistic action results in long-term damage, which is the case when decisions are vitiated by the lack of purpose and direction. In this sense I like to say simplistic notions of good and bad or right and wrong need to be replaced by a theory of error where they actually contrast the complete and the incomplete.

As our world becomes more and more complex and new forms of global interaction develop, decision processes also become more intricate and new approaches are necessary to open up the doors of the future. In sensing this, I continue working for better guidance that may serve not only this fascinating ground of Information Technology but every person who needs to understand the world and act in it.

Acknowledgements

I dedicate this book to my wife Jane Elizabeth Trigoso and to our children Robin and Isabel, thinking that my work may serve as a symbol of love in time.

This book would not have been possible without the continuous support of Professor Alan Guinn, Dean of Rushmore University, who read my small publications and encouraged me along the years to continue my research. At different points in this development, other Rushmore Faculty corrected my errors and helped with key ideas and approaches: Professor Laurence Leigh introduced me to the literature on decision theory, read several of my initial fragments and gave precious advice on various questions of economic theory. Professor Donald Mitchell helped me at a critical moment of my work by suggesting more study and new research methods. He provided me with invaluable references to the literature and encouraged me with my writing. Professor Mitchell also wrote an article describing my approach to Information Security, and our exchanges were useful for my own understanding of the subject.

Some of my first tries at the book were copy-edited by Ms Laurel Barley, the Rushmore University editor at the time I joined the Doctoral Programme. I will always remember her attention to detail and recommendations that helped me improve my writing. The present version of the book is, nevertheless, due to the guidance and infinite patience delivered by Ms Elizabeth Miller, our Rushmore University Editor.

Carlos Trigoso

Harrogate, United Kingdom

May - November 2012

Introduction

The nature of things is nothing but their coming into being at certain times and in certain fashions. Whenever the time and fashion is thus and so, such and not otherwise are the things that come into being. The inseparable properties of things must be due to the mode or fashion in which they are born. By these properties we may therefore tell that the nature or birth was thus and not otherwise.

Giambattista Vico, *The New Science*, 147-148

This work represents a systematic reflection on over 30 years of work in the IT industry and in particular in the Security profession. Many parts of the text were published in a fragmentary way since 2006 on my personal website, but the current re-worked text represents a coherent view and indeed a philosophy of Information Technology and Security which underlie all my previous publications.

The text is primarily addressed to Information Technology and Security specialists, but I hope that the general reader will still find an easy argument to follow. In fact, perhaps the core of my argumentation is that current Security and Identity problems cannot be solved and should not be addressed within the narrow and one-sided grounds of technology. I even think that most of these problems are caused by the unilateral view that technology is a cause, and not a consequence, of historical development. My thesis calls for a multi-ocular position, in the sense developed by the Japanese philosopher Magoroh Maruyama, where the techno-centric view is compensated and complemented by other perspectives.

I expect that a large part of the objections or misunderstanding that this text will provoke will come from my suggestion there is a global economic and social process that is reducing the relevance and finally will cause the end of the traditional IT Departments, both in the public and the private sectors. Challengers will focus on this more visible side of my assertions and perhaps ignore the basis of my work, which is a general theory and logic of organisation. Perhaps I should underscore here that, while I recognise the importance of Cloud Computing, I see it not as a technological phenomenon, but caused by business and social transformation. It would be wrong then to assume that I am some sort of "Cloud enthusiast" happily ignoring the practical constraints and realities of Corporate IT.

Confronted with predictions about the death of the IT department, and the scale of adoption of Cloud computing, people in the Computer Industry are sceptical. Things are not happening as the Cloud enthusiasts predict or want, they say, and the "defenders" of corporate IT may have a point indeed: the IT departments of the world are putting up a fight and are successfully delaying the next computing revolution. Nevertheless, this does not mean that traditional IT is being "successful" in the whole. Their

resistance is only delaying but not stopping the eventual realisation that corporate and organisational IT is not an intrinsic part, or a necessary part of business or organisational life, in any sector of activity. It became part of the common, standard organisation because of social and economic forces, and its fate is bound to the change of these circumstances.

I also would like to clarify what the next computing revolution consists of. Too often, Cloud enthusiasts (as well as their "enemies") assume the new computing platforms are the result of "advanced" or so-called "new technologies" that are changing how IT is done. This is an error, and for that reason I do not classify myself as a naïve proponent of Cloud computing. What has changed is not the technology, but the way technology is used. The reader should keep this in mind when reading this book.

A key test to see through both blind enthusiasm and IT regression is to analyse how the subject of Security in the Cloud is covered. While the Cloud proponents will minimise the problems around Security, the IT Departments will exaggerate the issues. I explain in this book that while there are problems – specifically around managing user access-- these issues are not so difficult and serious as the IT Departments would lead us to believe. Further, these Identity management issues cannot and will never be addressed with the conventional IT focus on technology. So it is a matter of seeing through these issues: those who never did Identity management well are speaking about an area which is foreign to their fundamental perspective!

By using fear and confusion, the IT vendors are not helping to clarify the situation and are in fact actively supporting the delay in transformation. They provide new versions of old technologies which serve to conform to the traditional organisational boundaries and to keep the conventional models of the IT departments. The public and private business and organisational leaders need to be careful when buying technology so as to avoid a path that will delay their business progress for years.

So yes, change will occur, perhaps not in this decade, not as fast as predicted, but change will come nevertheless. An index of this change is that expert consultancy firms –some of which I have worked for or with in the past decades-- are already adapting mentally to this change. As it becomes to our work, they describe the "options" and "modalities" of technology adoption. This is necessary and adequate. Our clients need to understand the options they have and should not be "sold" on some starry-eyed solution, but it is also our duty to alert our clients of the prospects. The global consultancy organisation Gartner made one such advance in 2011 when it alerted the IT sector of another shift in the Identity management space.¹

In the cited event, Gartner's Research Vice President Ant Allan, predicted that by 2014 "notable project failures" will cause 50 Percent of Organisations to shift Identity management efforts "to intelligence rather than administration." We didn't have to wait until 2014 to see this happen. I know that organisations across all economic sectors are moving away from the 10-plus-year-long trend to "manage" identities by means of automation technologies. This change was not direct, as first organisations moved away from "automated provisioning" towards "compliance solutions," wrongly

called "access governance." These in turn were able to address only part of the Identity problem, and now the trend is moving away from them too. The next orientation, which Allan calls "intelligence" is not well defined yet, but will focus on identity data management (identity analytics and data aggregation).

The "notable project failures" Allan refers to are not advertised in the press, but are nevertheless known to Security and Identity practitioners: global corporations either never implemented Identity management solutions as expected, or years of effort have come to nothing in this area. In this book, I analyse why this happened and suggest that the whole Identity management technology trend flatly ignored the organisational past and future roots of the problem.

While Gartner recommends that businesses focus on "monitoring, log collection, correlation, analytics and reporting,"² he also predicts that by the end of 2015 "more than 50 Percent of cloud-based IAM offerings will be hybrid solutions," i.e. a combination of on-premises and off-premises/hosted technologies and services. This is in line with what I propose in this book.

To foster change, an intellectual revolution is necessary, and it is essential to find the structure, the logic of such a revolution of the mind. What people inside and outside of the IT world need to understand is that things are changing in this industry, and are changing for good. We have the choice of becoming an obstacle or else lead the change. By change I mean that a new cycle has already started, whereby individuals determine what happens to IT technology--as technology inventors, producers and consumers.

Perhaps it can be said that the individual never left the scene, that large organisations were mostly "in the lead" during a long period. This was the period when organisations could "push" technology on the market, and decide what was in and what was out. It should not be forgotten, though, that the Computer revolution of the second half of the last century was a revolution of the individual and for the individual.

The future looks different to the traditional IT context where solution design and adoption depended on the producer. Now adoption depends first on the user. So Identity management services in the Cloud are inevitable, as corporations and organisations move to a situation where the "external users" are much more important than in the past.

People have been talking for years about user-centric security, but always taking the user as an enemy. In the old model it is always the "end user" who is not trusted. I am sure that this model is not sustainable even in the short run. User-centric shall mean the individual users and their teams, groups, affiliations, etc. will manage themselves and it will be up to the "enterprise" or the "organisation" to define the levels of trust and access that it will permit. There will be many levels of access. There will be more complexity, not less. Paradoxically, the "external user" will become more essential to the enterprise collaboration and more "secure" than the internal ones.

The essence of this book is that it breaks with conventional thinking about the idea of information and information exchange. At the base of my thinking there is a notion of bi-directional information exchange, and therefore a concept of Security where there is a bi-directional correlation of risk and trust: risk and trust on the side of the organisation, and risk and trust on the side of the user. My work then examines the ways in which we can abandon the ideologies prevalent in large organisations and allow the individual to assert his or her autonomy. At the professional level, I recognise there is a great levelling of all the professions and all the work activities, so that we all appear now as individuals in front of the corporations and state organisations. Persons are at the margin of organisations, –as Luhmann explained, and individuals are the economic and social abstractions that act within the organisation and interact with each other.

In the same way as this levelling transforms our activities, it also transforms our identities for each other and towards the organisations. It gives us less power as persons, compared with the abstract mechanisms of the private or public corporation, but it also gives us more power as individuals, as abstract entities. So I welcome this change, instead of seeing it as some lamentable "proletarianisation" of the professionals and workers, but the condition is that we recognise this process for what it is, instead of remaining immersed in the ideologies and false views that it creates.

If professionals, in particular Security professionals, lose autonomy as "advisers" or consultants, as proud independent actors in the industry, if our services become subservient in the present-day workplaces, on the other hand we can begin to understand that passive adaptation to this generic managerialism is not the only way forward. In fact, we have been there already, practising Security as one more managerial speciality, seeking standardisation and "rationalisation" as our only goals. We have also promoted "efficiency," "normalisation," and "universalisation," while suppressing conflict and dissident opinion. Aside of purging our professional lives of any sort of meaning, and beyond fostering a narrow technical rationality, where did all of this lead us?

I think of this book also as a sort of call to Security and Identity professionals to deeply revise ideas and abandon prejudices. As modern capitalism develops—in the only way it can—towards greater and greater abstraction of the individual, as it leaves behind the person with all its diversity and peculiarity, we should see this also as a moment where we re-assert ideals of completion and purpose beyond and outside "business as usual." Yes, we have survived the transition from the personal engagement of the professional, the "trusted adviser," to a context where the rule is that "nothing is personal." What remains of the person then? How do we express the ideas of person, individual, belief, intention, identity, responsibility in the current context? What is the purpose of organisational know-how and professional choices?

Computer Security—as I show in this book—is now universal but is also "hollow." It is "valid" but also empty of particularity. This happens because Security is a dependent activity inside a much wider set of determinations. So, I address Security and Identity in a search for completeness that takes me outside of the conventional boundaries and technological thinking. I hope the reader also sees that it would be

fruitless to discuss Identity and the related subjects in isolation. Because Identity management sits "at the bottom" of the symbolic chain that starts with history, sociology, economics, business, management, IT and Security, any valid assertion about these—more general—spaces will also be valid for Identity management. Contrariwise, a valid assertion for Identity management is not necessarily valid for the upper, more encompassing realms that surround it.

Therefore, it is not possible to address the issues of Identity and its management without transforming our thinking in all the other areas of organisational and business activity. This explains the large variety of subjects that I discuss in this book. Throughout the text, the reader will see there is a strong emphasis on systems theory, and the idea of organisations as "articulation of differences." Equally strong is the notion that the fundamental logic of the organisation is a distinction between members and non-members of the same and that "communications" are driven by distinctions. Also, the evolution of such distinctions is the key mechanism of change in organisations of all classes. Following Luhmann, I think that an organisation does not exist as a metasystem of the individuals it encompasses, but as a system in its own right, a self-differentiating network of communication.

In this sense the maturity of an organisation is reflected in its internal division of work and strands of specialisation. This increase in differentiation does not need or imply a greater or better degree of inclusion of the person, or a more complete or "ethical" mode of action. In fact, the organisation becomes less humanistic but simultaneously more universalistic the more it develops and differentiates internally. This in turn means that the decision processes are less complete in the sense that these become more "managerial," more one-sided and short-term orientated. This happens in paradoxical fashion against a backdrop of increasingly detailed and specified rules, policies and procedures, industrial standards and regulatory frameworks.

The key insight of Luhmannian sociology is the organisation is not a thing, a continuous entity, an addressable unit of nature which owns its information processes and hence may decide how to use or manage these resources. The question is, if such a communication exists that will result in a differentiation of practice (a "new" practice). Even with a conscious decision towards new standards or solutions, we need to remain aware there is neither a guarantee nor a causal relation that decisions are either rational or sustainable. Decisions, as taught by Luhmann, are communicative acts within a network of informational exchanges; therefore, decisions are always contingent.

This theory allows us to see Security as a communicative act whereby assertions of risk and trust are made because these become operationally necessary in organisational life. An additional slant is that risk is contrasted to trust, as if it were a separate idea, only because of ideological constraints. The Security professions "differentiate" themselves in the network by stressing the discourse of risk and this is what explains the predominance of this thinking, not the other way around.

Against this trend, I show how the discourses of Risk and Trust are co-dependent and correlated, and how the conscious professional can step back from the easy "differentiations" that lead our professions

down the barren path of Risk Assessments. In the context of organisational discourses, because the organisation excludes the person, we cannot speak of a "bounded rationality" or certain "limits" of human thinking. This would assume that a full or complete rationality is possible for the capitalist organisation or the modern corporation. In reality, without the Person, in a network of abstract individuals we can only have partial discourses based on the fragmentation of activities, the "specialisations" and the constraints imposed on the individuals. "Error theories" arise from these sub-rational (not "irrational"!) discourses, not from the choice process or the psychology of the people involved, but from the inevitable constraints of individuals acting in an organisation.

In chapter one, "Security as a Problem," I show how Security is not the obscure and boring area it seems from the outside, but a practical discipline fraught with issues and challenges. While it occupies a seemingly well-established space in the IT world, it lacks a theory of its own and is dependent on decisions and ideas that come from outside of it. Security professionals have to see our area as a problem first, if there is any hope for change.

In chapter two, "Freeing Security from Risk Avoidance," I address the dominant ideologies of Security and Risk Management, explaining how these form a one-sided view of reality. I also show there is a fundamental flaw in this approach, by which the Security practitioners have confused objective with subjective risk and misinterpret standard probability theory.

In chapter three, "Security and Information: Access Management," I revise the basic concepts of Identity Management and Security. Elementary definitions of "access control" are developed first to then understand what access control means in the context of business and public organisations. In this chapter I also redefine Information, explaining the current preference to see Security as an object.

In chapter four, "Identity becomes Data," I show how social and economic transformations are homogenising identity exchanges. This in turn moves the task of controlling identity and access to a form of data integration and management. This global transformation is the ground on which we have to rethink all the areas of Information Security.

In chapter five, "Identity Services and Programme Delivery," I detail the current problems faced by IT and Security projects and how these reveal one-sided definitions and wrong expectations. Identity management is part of a general trend marked by failure and frustration in IT management.

In chapter six, "The Cloud Transforms the Network," I offer a wider perspective of the more recent changes in Corporate IT and the next Computing revolution. I show how "old" and well-known technologies are used in a new way by a rapidly growing user population and new models of organisation. Social and economic transformation changes the space where Security professionals have to define their purpose.

In chapter seven, "Quantitative Identity Management," I introduce new criteria to understand information as data exchanges within the organisation. The crucial concept of interaction of identity and business data is explained, to show how we can begin to develop a Quantitative approach for Identity management, moving away from the previous focus on Risk.

In chapter eight, "When is a System Secure?," I review the current status of data protection and the failures of Security management. I demonstrate that a change of direction is necessary to centre Security strategies on the exchanges, the processes of communication where value is created.

In chapter nine, "Persistence of Techno-centrism," I explain the views focused on Risk, Protection and Technology are not transient and will always be part of the organisational discourse. While this remains true, I call on the Security professionals to adopt a wider, complete view of the organisation and recognise the various logical perspectives that are at play.

In chapter ten, "The Cloud Transition," I return to the analysis of the current period of history, and describe the potentials and pitfalls of the adoption of Cloud solutions. In particular for Identity management, the Cloud Transition offers the possibility of finally setting up this speciality in its own rightful place.

¹ "Gartner Predicts By 2014, Notable Project Failures Will Cause 50 Percent of Organizations to Shift their IAM Efforts to Intelligence, Rather than Administration," Gartner Identity & Access Management Summit, London, March 2011 March, <http://www.gartner.com/it/page.jsp?id=1540014>

² See also my 2006 article where I propose an integration Security Information model: Carlos Trigos, "The Path to Assured Solutions," <http://carlos-trigos.com/public/the-path-to-assured-solutions-original/>

1. Security as a Problem

Approach to Security Management

This book brings together many years of work in the IT and Security industry in public and private organisations. My experience and research have revealed several interlinked problems that result in low quality and performance levels in security investment decisions and project delivery. An important goal of this work is to show the complexity of interrelations, calling for a systemic view of the situation. I approach IT Security Management as an organizational and sociological problem with a dense network of interacting processes. This network is characterised by “negative feedback” chains,¹ interactions that have negative, self-sustaining vicious circles. This type of interaction is present in the whole of IT management, but has particular relevance for Information Security and Identity & Access Management.

The concept of a “negative feedback chain” or “negative causal chain” is generally associated with the disciplines of System Dynamics,² but it can be applied to any area of science. Identity & Access Management, one of several disciplines in the IT Security arena (alongside Cryptography, Network Security, Operations, Applications, Continuity and I&AM) is the one that most affects organizational, non-technical concerns and at the same time the one that is most affected by factors not dependent on “technology.”

Although organisational features affect the development and adoption of Network Security, the actual changes in this area do not affect an organization widely and tend to remain “in the background.” Identity & Access Management directly induces changes in the organizational structure, and requires specific changes, without which the identity processes cannot even start.

Identity & Access Management requires the principle of Identity Data Ownership and Custodianship, for example, without which it is impossible to define, validate, and re-certify any access control model. Without these, in turn, none of the other advertised benefits of Identity Management (e.g. agile user provisioning) can be materialised.

The Identity & Access Management process also introduces changes, in that it creates new processes for authorization, maintenance, and termination of user accounts. It does not matter, really, if these processes are automated or not. What matters is the processes are in place, and these are mandatory, standardized, and efficient. From a different angle, Identity & Access Management demands certain disciplines on IT project definition and execution, especially in the way user data is stored, updated and transported between systems.

A systemic approach to IT Management and Information Security decision-making requires planning and analysis of the organizational changes that are necessary for a successful outcome. On the other

hand, organisational resistance to change is the main obstacle to Identity & Access Management as a business process.

Considering the negative feedback chains here described, it is essential to promote change to explain and modify the mind-set of the stakeholders and interested parties. Above all, it is essential to reduce uncertainty regarding organizational transformation and to show the need for a higher, more complex organizational model.

The changes implied by Identity & Access Management affect each one of the employees, temporary workers, contractors and consultants, partners and service providers in an organization. They also affect and extend to the customers and the public in general. In my experience, then, getting organizational changes right is the key to designing and implementing Security Management and secure Identity processes.

The Need to Discuss Security

For many years, it was almost impossible to discuss the principles of IT Security in professional circles. Even as late as 2005, it was seen as a scandal to mention the severe limitations of the IT Security specialities. The general, dominant assumption was that IT Management and IT Security were self-evident scientifically “true” propositions.

Something in my personal history, perhaps my heterogeneous and discontinuous experiences in life, led me nevertheless to have a sceptical view of technology in general. I was first an IT user during a period as academic researcher in the early 1980s, and then moved gradually through many of the technical and business areas typical of Information Technology: developer, integrator, specialist, vendor, architect, trouble-shooter and consultant in a career spanning 30 years to date.

Only after many years of work, did I begin to organise separate observations about my professional activity, and it became clear to me that overwhelming confidence in technology and lack of insight were in many respects similar to an ideology. The late works by Theodore Roszak were particularly educating in this respect.³

In Roszak’s definition of these ideologies, nobody is responsible but also nobody is free, as an overarching imperative guarantees the goodness of technical progress. Even when an organization is damaged by technological mismanagement, there is no problem. Everybody is doing the best they can in a general movement of progress towards further and further adoption of technology and science.

My personal view increasingly became —that we should be instead asking why we do not seek completeness instead of “progress.” This was especially visible in the 90’s, when the IT world was struggling with the push towards alignment between businesses and conventional IT practices.

From the point of view of business management, starting with successive monetary and economic crises at the end of the 20th century, it became less and less evident that more technology was the

answer to any problem. Nevertheless, the expected alignment never was completed and even today the fundamental problem in every IT department is an almost complete alienation from the business direction.

In this context, proposing a conception of Security beyond or without technology was always received with derision and even disgust in the private circles of IT consultancy, especially in those more focused on the intricate technologies that came with the World Wide Web.

In spite of a general techno-centric slant and long resistance, it is now becoming a shared truth that Security is an organizational problem. Identity Management, in particular, as I like to say, is approximately only 5% technological and 95% a question of organizational transformation.

Why does security fail?

Another approach to these problems started with research on the causes of IT project failure. It was an advantage for me to move across several IT specialties and technologies, as well as many private and public sectors, because this allowed me to see the common factors at work.

I have arrived at a notion of IT failure or success as a measure of lack of change. IT Security fails because it comes last, because it is limited to technology, because it is reduced to compliance, risk management, and protection. These terms will be explained in full in the following chapters.

Technological belief in “progress,” defensive reasoning, ideological thinking and action, and unconscious behaviour doomed IT Management and Information Security from the beginning. There is a spurious alignment of IT security by which it makes people focus almost exclusively on risk management (risk “reduction”), so that Security becomes synonymous with “perceived secure operation,” and risk becomes synonymous with “perceived risk.”

In the same way that microeconomics should be studied in the context of national and international economics, Information Security should be understood in the frame of IT economics, and IT economics should be made dependent on microeconomics arguments. In this sense, Security decision-making operates on a dependent, derivative group of technologies and disciplines. Moreover, Identity Management is in turn doubly dependent as it is itself embedded in Information Management in general.

Bound by these circumstances and devoid of a proper link to business decision-making, Identity Management becomes a reactive, administrative discipline. For the same reasons, Security ends up as a discourse of exclusion, control, monitoring, and retribution. I sense these perceptions will soon be widely accepted.

All errors derive from wrong methods, but no method can guarantee the intended results. A well-founded method is one that is complete, one that balances theory and practice and, essentially, all aspects of a problem. An error is usually defined as a decision that leads to a loss of something valuable. In practice, though, good decisions may lead to negative results too, and good results may be

attained by flawed decision methods. This arises from the nature of decision-making, as the results of an action depend on the purposes of the decision-maker, and not on the procedures followed.

To achieve good, satisfactory results, a decision has to be complete, covering all the perspectives of action. Decision methods must be judged not principally by their results in a specific instance, but by correlating methods to purposes.

Human action is completely determined by partial knowledge, and fundamental sources of uncertainty are human actions themselves. While we can seek to reduce uncertainty and risk with decision procedures, we cannot eliminate it. When we decide, we necessarily accept uncertainty, take risk, share risk, and assign trust to other participants in action.

This principle is present in IT Security in a most elementary form: almost all Security disciplines are predicated on access controls. It is assumed that good security is equivalent to a framework of policies and measures to keep unauthorised access from occurring. Thought outside of this conception is very rare.

This work addresses the problems of decision-making in Security and Identity Management in the context of business and organizational transformation. To date, Security disciplines have been dominated by a focus on “protection” and “access control” with a secondary focus on business models and strategies. This is why we need to redefine IT and Security management.

The Missing Discourse

My work focuses on the critique of techno-centric discourses in IT and Security management. These “mechanistic” discourses arise from a long period of explosive adoption of electronic computing.

I see two main “discourses” operating across the IT professions: the discourse of Risk Taking and Trust Definition (or the discourse of the owner), and the discourse of Risk Avoidance and Trust Enforcement (of the discourse of the technologist). A partial analysis of these discourses can be found in some of my previous publications.⁴

A key finding of my research is though, that while these two discourses are “present” in every aspect of IT management, the current dominance of technological ideologies causes a very specific transference of responsibilities from the “asset owners” (the legal proprietors) to their managers; and from these to the “experts” (the implementers of the technology).

This transfer of responsibilities appeared on top of the historical ascent of the managerial classes early in the 20th century, but then accelerated as electronic computing substituted many productive functions and created new layers of managerial workers. The producer became a mediator. The problematic discourse that dominates Information Technology is present in other areas of organizational life and business, but it is particularly clear in IT and Security management through the serious problems it generates.

The most interesting result of this double transference is the lack of a discourse of ownership across all levels of the enterprise. This phenomenon has been observed recently at the level of business management, with the prevalence of “absentee” owners in the banking sector, but the same phenomenon is present at all levels of the organization.

In IT and Security management, there is a “missing discourse” characterised by the fact the “business operator” or manager can and may only act as a representative of the owner, but only in a formal capacity and never as a real, committed proprietor of the business.

It is my aim to show how the lack of the “discourse of the owner” has incalculable consequences for the planning, analysis, design, and implementation of business programmes and in particular in IT and Security management. In essence, what we see is the absence of a discourse of the owner, or the Master Discourse,⁵ as the lack of ownership is the primary catalyst for all organizational failures and for the permanent unsolved problems in Information Security and IT in general.

The absence of the Master Discourse is an absence at the level of experience, but not at the level of the structure, because the discourse of technology (“science”), in the foreground, actually presupposes the discourse of the Master, mimics the discourse of the Master, and responds to all challenges speaking in the name of a Master that cannot be seen. There is an extreme level of faceless technological control, executed according to a series of assumptions but where no single individual takes ownership. This in fact means that nobody takes responsibility for failure and all “progress” is illusory.

This state of being can be described as also a situation where truth is unspeakable, not only because it is psychologically hidden or negated (as rooted in the absence of the Master), but also because it is quietly but effectively banished by corporate and “professional” ideologies and structures. Secrets become lies, and lies become secrets. The differences between seeming and being are inverted and reflected through the chain of discourses.⁶

In this context we can speak of a world of “hostile cooperation,” a Hobbesian state of “all against all” in corporate life. This state is not necessarily malignant, as it arises from natural conditions of human society, but many consequences are negative. The essence of this state is that cooperation exists only when there is negotiated advancement of the “consensus.” In practice that means there is effectively an obstacle to actions not signed by the promotion of private, subjective “interests.” The human person does not have a place.

At a different level, this can be conceived as the prevalence of incomplete action, where the dominant actors and their intermediaries work only to control waste and loss with very short-term goals in mind. A wider analysis of these matters could lead to a critique of capitalism, or more precisely of the contradictions between some forms of capitalism and how these become obstacles to the development of regional and national markets. It must be emphasised that, in any case, incomplete action and short-term capitalism are consequences of the loss of personal context and social coherence.

What does this have to do with IT management and Security? As I will show in this book, there is a top-down causality in our professional activity, determined first by history, then by economics, and only by technology at the end of the chain. For example, if we propose the need for a balance between the discourses of risk and trust (risk taking and trust enforcement), we soon have to recognise these positions are made impossible due to the lack of the discourse of the Master. This absence has nothing to do with IT or Security. It is rooted in history and economic structures.

This is another way of saying there is an increasing complexity of business and life in general, and that no phenomenon can escape these processes. Techno-centric ideologies tend to assume they are free from historical factors, but that is precisely the symptom we need to address.

In the past “progress” meant a development of the division of labour, i.e. new technologies, which were practices of social groups differentiating themselves in the context of society. There was a sense that social and technical developments were interdependent and supported each other. Today, that sense is lost and may never be recovered.⁷

Global Trends in IT and Security Management

The general trends transforming business also transform Identity and Access Management. This has to be thoroughly understood so that we do not continue thinking there is some intrinsic value in “doing” Identity Management. It is not intrinsically better to apply a “trust management” perspective than focusing on “risk management” as in the past. The reason for this is that Identity Management is completely dependent on the fate of IT as a whole, and this in turn is entirely subsumed in the direction business may take.

Overarching and global trends will determine what happens with Information Security and Identity in IT:

- The protection and compliance focus, which Identity Management inherits from the Security Domain, will not disappear, but it will have a lesser role than it has now.
- Centralised control models over identities will be reserved for very restricted areas of the IT infrastructures, while at the same time organisations implement federated and decentralised assurance services.
- Privacy and Data Protection concerns will be seen as essential, but increasingly not as a central management task and instead as based on the individual choices and different varieties of identity.
- Identity Management as a service will experience rapid adoption, but a single model will not exist. Organisations will have partly hosted and partly on-premises solutions.
- The intellectual structure of Security and I&AM will change, moving from a focus on Risk Management, to a balance of Risk and Trust Management.
- Security will rely even more on defences in depth, a variety of identities and identity assurance levels while deploying risk-based and attribute-based controls.

When considering the future it is essential to look beyond the IT disciplines. Identity Management in particular needs to stop thinking about itself, and stop producing more and more detailed sub-specialities and taxonomies for user administration: provisioning, access, roles, governance, or compliance. Looking beyond itself means setting its direction in accordance with wider aims at the level of the economy, industrial sectors and specific business operations.

If we seek the links with higher and wider economic and social goals, we rapidly find there is a fundamental problem, rarely recognised in professional circles. The problem is the lack of a Security Theory. In other words, we have only “models,” “principles,” “frameworks” and “best practices,” but no theory at all. Better said, we have a situation where Security theories are implicit, in the form of assumptions and presuppositions, but are untested or just taken for granted. These principles and assumptions are embedded in well-established professional training manuals and technology documentation. One very visible case is the overwhelming prevalence of the definition of Security as risk management. This has remained unchallenged for many years, with very few exceptions.⁸

Contrary to the dominant ideology, my work in Security and Identity Management is focused on innovation and change. While this emphasis is essential in business in general, this is particularly relevant for Security. I see it as my mission to work with experts and clients, sometimes against conventional “wisdom,” analysing the problems in depth and bringing in new approaches and understanding.

I focus my message on conceptual integrity and completeness, and my goal is to offer a coherent view and strategy that makes sense for business leaders, government institutions and the public in general. It is my experience that too frequently organisations are affected not by lack of knowledge, but by lack of forward thinking and anticipation. This is particularly the case in the Security arena, where professionals tend to be “defensive” and “static” with the consequence that they end up resisting change and improvements.

I developed the approach presented in this book throughout many years as a strategist and troubleshooter for major information technology organisations. I found that few problems in the Security practices arose from technological causes but from the uses of technology, especially from organisational factors. In response to this, I formulated a systemic solution method highlighting the blocking factors in the organisation first, and addressing the technological levels second. Many organisations still have difficulty in seeing Security as part of the Business Model, or as part of their information management strategy, but the moment is coming when a Security Architecture will be an essential part of corporate strategy.

I propose a coherent model encompassing four Security disciplines, those of Direction, Selection, Protection, and Verification. This is my model of “complete action” in the Security Arena. Developing this model is my central motivation in writing this book.

Theories of Error

Contemporary management practices are “theories of error.” They can be rightfully called so in two senses: first, because they are ideologies purposely constructed for the management of failure, and second, because they are impervious to error. While on the surface these theories appear as reasonable technologies to control the outcomes of human organised practices, in the course of their implementation they become little more than justifications for limited action if not even theories of how limited, incomplete action can be passed off as successful.

Management Theories present themselves as technologies of resource optimization, as well as success-oriented and excellence-seeking methodologies. Ideally, management covers various aspects of human action:

- “Delivery” – Here the concern is how I deliver change to the business quickly and cost-effectively. In IT, this means getting technology investment under control and optimizing it by avoiding waste and inefficiencies. The ultimate goal—still unattained in the whole—is to align technology investment with the business strategy.
- “Change”—Here the concern is to ensure that technology is an enabler for organizational change. The question is how to use technology to facilitate change, while reducing costs and exploiting opportunities for capital accumulation.
- “Implementation”—Here the concern is to minimize technical risk for service delivery. The question is how to ensure timely and economical technology solutions that are fit for purpose and correspond to expected standards.
- “Budget”—Here the concern is to manage investment and expenses so as to ensure these support and maintain profitability at least or preferably increase the profitability of capital. The question is how to exploit technology so that investments are controlled, fully exploit previous investments, and deliver the expected financial results.

Looking into these requisites of business management, which are applicable to IT and Security, I often call for a balanced approach. These four principles all have to be present in a good Security Management initiative. Nevertheless, it is also true that Security by itself cannot reach such a balance because it is a dependent discipline, a subsidiary of other levels of management. All the limitations and intentions present in business management express themselves in Security Management.

What we find in the market is that, on the whole, business managers are frequently making sub-optimal or even wrong decisions in respect to IT and Security. The negative experiences in Identity Management are particularly serious. It is therefore necessary to develop our professions to face up to and resolve these problems, which rise up from the passive and techno-centric advice that is now prevalent. It is valid to ask in this context if business demonstrably suffers because of limited, incomplete decision processes in the Security space. Some specialists tend to think that decisions may well be wrong from a security perspective but not lead to any negative outcomes outside of their perception of acceptable risk. In that case, are such decisions actually wrong?

What would you think of a multi-million Pound Sterling investment that sits on the shelf for years while the customer pays maintenance for a system that never was implemented? Is an investment intended to enable regulatory compliance that was never delivered and was instead replaced with additional investment on custom software not a failure? What can we say about a choice of technology that does not match roughly 90% of the business requirements? What would you call a solution selected after it was rejected by three successive technical evaluations or Requests for Proposal?

Perhaps some would argue that stretching things, we could say that organisations are taking their fate in their hands and assuming some risks; or perhaps they are willingly going into such situations and therefore assimilating some specific costs for some specific risk levels, but surely that is not very satisfactory. The real solution to these problems lies in having the ability to estimate the economic outcome of IT and Security decisions. For each of the bad decisions mentioned above there are evident financial costs:

- The costs of paying licences for an unwarranted technical choice.
- Wasted time and effort in technical assessments that are subsequently ignored.
- Additional investment required for remedial work to substitute the failed implementation.
- Additional risks incurred by delaying regulatory compliance.
- Additional costs caused by the perpetuation of a bad security arrangement for years on end.
- Productivity losses due to complexity of the manual operation of the system and excessive use of personnel for security operations.
- Wasted effort in developing in-house solutions (custom code) that will have to be discarded when the security system is implemented.

Similar examples of waste, over-spending, mismanagement and increased risk, cost and disadvantage can be found across the IT and Security market. It is not a matter of being or not being a security "purist." The management errors are too evident and numerous to be ignored.

While the formal, "final" decision is a business matter, and while the business executives carry the responsibilities arising from those decisions, IT and Security experts need to be able to recommend the best decisions from an economic point of view. Not doing so, and taking refuge in the notion that it is not our problem, is a dereliction of duty. We need to speak the language of business and operate under business, capitalist criteria. The language of business is a financially-centred, calculation-based language. It is the language of economics. We need tools to measure security investments, in the same way as we measure other aspects of the effectiveness of our IT strategies.

Following this, it makes sense to review the concepts of information, system, organization, security, and identity to make sure they correspond to clear micro-economic ideas. Too frequently, we take these concepts for granted, but on closer analysis, it is not self-evident what we, the IT experts, understand by information, or by systems security. Therefore, it is necessary to define these terms.

To begin with, we need a definition of "information," not a general one, but one useful for information security. Information security is not an area unique to itself. It is just another business concern,

comparable to Continuity Management, Availability Management, Configuration Management, and other related processes. If it appears as something "different," it is only because of historical reasons. There is still some trendiness in seeing Security as something special, but nothing stops us from evaluating Security strategies and investment decisions in the same way we assess any other business financial and operational process.

So far, my focus has been to point beyond standard risk-based analysis, not because of a desire to negate the importance of risk analysis, but because of the specific goal of investigating how investment decisions are actually made, with or without risk analysis, and independently of the depth and quality of it. As probably all Security professionals have experienced, risk analysis and risk management constitute only one more factor in the investment decision process, and do not seem to be very effective in guiding investment decisions.

Years ago, while working for a global consultancy firm, some senior managers told me there would be very little attention paid to my research programme, and that I should dedicate my energies to something different. I didn't find that discouraging. It actually showed how serious professionals can become trapped in a haze of self-sustaining ideologies, until it is too late and everybody suffers from the lack of alternatives.

We can only become better professionals if we understand the context of our efforts. How is a Security strategy designed? How are investment decisions made? What is at stake? What is really our purpose when devising an Enterprise Architecture?

Enterprise Architecture

Around the same time I was having such debates, I started following the work of John Arnold, a British Security Architect. In 2006 I adopted some of his categories for Security strategy summarised in the principles of "Select, Protect and Detect."⁹ As part of the Jericho Forum, John Arnold has made very important contributions to the theory of Collaboration-Oriented Architecture or COA.¹⁰

Arnold addresses directly enterprise architecture as "collaboration-oriented." Many types of organisations are already in a position where the only approach viable is "collaboration-oriented," beyond the old security style based on "containers and perimeters" defined by either "letting you in or keeping you out."

Arnold correctly identifies the current trends in mobility and agility, de-perimetrisation, outsourcing, cloud-based solutions, demand for scalability and more complex access policies.

On the other hand, while the COA approach makes full sense of these trends, it still does not address the investment decision process at the economic level.

As Arnold explains the term "collaboration" generalises the concept of "contract," as being an agreement with elements of offer and acceptance, a price, criteria for legality, and mutual understanding of what the contract is about. This is a good approach and I believe this should be

exploited fully. To deepen the notion of collaboration contracts, it is necessary to consider relationships between rights and obligations as well as those between liabilities and immunities. I will cover this in a chapter of this book when discussing the theories of W. N. Hohfeld.¹¹

Beyond these points, perhaps the most important concept proposed by Arnold is that of a "lifecycle of the collaboration" (Search, Negotiation and Fulfilment and Termination), because it maps to previous work he did around the notions of Elect, Protect and Detect as indicated some lines above. Sadly, these older concepts are not clearly present in Arnold's recent work. I have based my model on an extension of the ideas of Elect, Protect and Detect, and I explain this in a separate chapter under the theory of the Security Perspectives (Direct, Select, Protect and Verify).

Adopting a wider conceptual framework, as Arnold has done, links Information Security with business and economic considerations. Technology moves to the background when the goals and principles of Security are determined primarily by the microeconomics (more precisely by capital profitability and capital investment decisions).

In spite of the positive aspects that I note here, Arnold's work does not bring a new answer to the definition of Trust. Arnold explains, "collaborations create rights and obligations and that trust is an essential precondition for collaboration among people and organisations."

In my view, this is only half of the reality: trust is also a post-condition, in the sense that trust is "defined" at the beginning of the collaboration lifecycle, but then has to be established, enforced, and monitored. Therefore, it is not an ingredient that comes first but a permanent facet of all corners/sides of the trust lifecycle. My own work on this matter shows the four sides of this process.¹²

Also in my view, risk is intrinsic to the trust lifecycle and runs in parallel to the instances of trust management: for example, for the instance of "trust definition" there is an immediate correlation, which is "risk-taking."

A conventional approach to risk is one where it is inherently statistical and negative. Risk is associated negatively with "events" and "actors" which affect "assets." I would suggest that risk arises also from risk-taking decisions of the decision makers; hence, it has positive values in at least three moments of the four we can see in the collaboration lifecycle.

Arnold's "Trust Process" or collaboration lifecycle lends itself to a close mapping to the four-fold model of Trust Definition, Trust Allocation, Trust Enforcement, and Trust Monitoring that I have been developing in the past six years.

The steps proposed by Arnold can be mapped as follows:

A) Need Identified + Searching + Potential Partner Identified = Trust Definition

B) Negotiating + Collaboration Agreed = Trust Allocation

C) Fulfilment + Resource Access = Trust Enforcement

D) Fulfilment Events + Analyse Performance + "detect good or bad performance" + Manage Reputation = Trust Monitoring.¹³

The best aspect of Arnold's work is that he sees organizations as collections of collaborations. This is precisely the outcome of an era of globalization and transnational capitalism together with extensive utilisation of electronic computing and commerce. Arnold notes that current Security tools and architectures aim at securing "individual" accesses. He is fully right in understanding that this is fundamentally wrong, and defends the need to make access control decisions at the level of a complete partner-to-partner relationship, i.e. a collaboration agreement.

I believe that this approach is the root of many improvements in IT and Security management, perhaps going even beyond "collaboration-oriented architecture," addressing what Security should be in a very wide sense. Thanks to this approach, security itself becomes collaborative, insomuch as assurance levels, access routes, processes and data governance are defined and managed outside of the limited box of the traditional techno-centric management.

Wasting Time in an Impossible Mission

"Wasting time in an impossible mission"- that common sentence summarises the actual state of affairs in the IT sector, perhaps more for the user side of it, either the organizations using IT systems, or the end users, as either employees, citizens or consumers.

Some so-called "new" approaches to Security have tried to explain what is happening, by saying that behavioural aspects have been underestimated,¹⁴ but we would need to go deeper to reveal that no amount of clever "behaviourism" will resolve the problem if technology continues to be the focus of our profession. Let us be frank: in many cases, we continue overvaluing technologies that are actually part of the problem.

An extreme view of this exists, represented by philosophers who have identified the mere use of technology as a threat to human culture and being.¹⁵ My position is not extreme in this sense; as I do think there are technologies (as I will demonstrate in this book) that can readily address the problems here discussed.

Technology guarantees uniformity, standardised futures, says T. J. Rivers. We see the world "in need of alteration,"¹⁶ and act upon it not on principle but on circumstance. This may be true at one level, once the technological cause is already established in the world, but it would be an error to see technology as "the" cause of the loss of human purpose. Contrary to this, I see technology as a product of people transformed by capitalism, not capitalism as a product of people transformed by technology. More critically, capitalism itself is a product and not the proverbial "structural cause" of all the problems of humanity.

In a pre-capitalist and "cultural" era, human actions arose from personal, family, tribal, and ethnic context, while in late capitalism "being" (using River's terminology) appears as arising from human activities ("actions"). I would add precision to this by saying that current human activities, in the post-

cultural era, are partial and incomplete, and in this sense they are “technological,” i.e. devoid of context and content, generic, global, a-cultural if not even anti-cultural. This historical envelope is characterised by mass-dispersed mediocre activities that are nevertheless pragmatic and normal. Not a disease, but the necessary product of a wandering globalised humanity.

There is nothing wrong in seeking the perfection of technology if we fully understand that it is the product of a previous loss, the loss of complete human action; but the key is that we see technology for what it is, and we use it with cold comprehension and no illusions.

After all, electronic computing technologies are wheels and cogs in a universal machine that is the harbinger of a global post-cultural world where the only danger is that we continue believing and following new monolithic ideologies in place of the old ones. We should stop being driven to whatever technology says is possible, and technology needs to be challenged to achieve freedom and purpose.

Information Ideology

In 1986, Theodore Roszak, one of the original philosophers of the new technical era, nevertheless denounced a “new ideology, the ideology of computer technology and information science which has become almost a new substitute religion.”¹⁷ He called it “cyberism,” the cult or creed of information.

Roszak understood the key premise of cyberism “is that information and technologies connected with it - notably the personal computer and the home television set - are creating a new social order. The data banks and the smart machines - not the working classes, not the intellectuals of academia, certainly not the politicians of the capitals and the courthouses - are now being heralded as the true drivers of revolutionary change. This is the core belief around which all the other elements have grown - opinions about everything from economics to human nature - which it takes to build an ideology.”¹⁸

I equate Roszak’s “cyberism” with the Mechanistic Perspective in Information Security (as I explain in this book), entirely relying on machines and processes to “handle” information. This perspective assumes that information can be conceived as an object in itself, as a flowing substance which is objectively, physically valuable.

The Mechanists unwittingly support and are supported by an ideology that is geared towards the reign of technologies and the use of technologies for the sake of it. On the other hand, this is not only the position of the technologists or IT experts, but also that of technology vendors and many consultancy firms.

W. Truett, commenting on Roszak’s work, writes, “For cyberists, information is not only a political force; it is also the new economic power that supplants or transforms all the other forms of capital.” Daniel Bell, one of the first of the information theorists, called information “the strategic resource and transforming agent of the post-industrial society,” the central pivot in a “new social framework based on telecommunications.”¹⁹

Cyberism –as noted by Truett and Roszak-- the "idolatry of information" --extends into politics, business, management and all human relationships. For example, private and public management skills, as taught in management schools, are unthinkable without reference to "information technologies."

It is in this context that I propose to investigate what IT management is and what Security means in that frame. Not doing this, accepting the given truths of the information age, would most decisively disallow any change and any hope of finding new ways for our professions.

My long experience in the IT world has convinced me there is a deep, pervasive, persistent, ingrained cause of error and failure in judgment and that business planning cannot be practiced outside of a coherent philosophical understanding of human nature and history.

Philosophical work is not common in the techno-centric world. It is sometimes rejected without a thought, but I never found a valid reason for not thinking philosophically about my own practice.

A good approach is to start by revealing the metaphors and paradigms that operate in day-to-day IT Management and Security thinking.

The "root-metaphor" theory of S. Pepper²⁰ and Hayden White²¹ is very useful to organise a review of the IT world as a whole, and most of my work in this area is indebted to these thinkers. For example, I mapped the trends found in IT and Security to Pepper's four "root metaphors."²²

Similar very powerful approaches are those of G. Morgan and G. Burrell²³ and H. Dooyeweerd.²⁴ A more direct approach to paradigmatic analysis is that of Klein and Hirshheim, whose text should not be missed by any IT practitioner.²⁵

Every human endeavour has an element of error, due to uncertainty and "natural" uncontrollable factors, but more deeply analysed, we can see the central element of error, beyond circumstances and accidents is the tendency towards "self-serving cognitive distortions" or "cognitive conceit."²⁶

This is precisely what I have found in my experience and the analysis of IT and Security strategies and decisions: we can see the coexistence of multiple "paradigms" and "metaphors" at play in corporate/organisational life, and how these tendencies affect investment and design decisions.

This analysis also shows how the philosophical motives of these tendencies (usually unconscious) control the ideologies at play in all spheres of business and technology.

I do not think that every error or every problem can be reduced or should be reduced to the "noetic effects" of the underlying paradigms, but this principle certainly illuminates the way forward. My investigation will show in some detail how we can make sense of error in such a specific area as organisational decisions and security investment, why error and failure in judgment are so persistent, and why organisations fail repeatedly in their choices.

Unilateral thinking bound to one or the other paradigm stifles human reasoning, but not absolutely, not totally. This tendency affects us less when we operate at the level of the empirical, the numerical or arithmetical, but its effects become overwhelming when we need to think about purposes, strategies, and longer-term durations.

Moroney quotes theologian Emil Brunner: "the more we are dealing with the inner nature of man, with his attitude to God, and the way in which he is determined by God, it is evident that this sinful illusion becomes increasingly dominant."²⁷

Let the reader not be distracted by the reference to religion in this context, as this is just a way to understand, to express purpose. There is no philosophy without purpose, and purpose does not need to be religious. Both believers and unbelievers will have had the experience that it is much more difficult to ascertain truth when we are dealing with "the inner nature of man" (i.e. with the personal, contextual nature of the individual), than when we deal with consensual, socially shared objects.

I am painfully sure that unethical thinking, opportunistic marketing and failed strategies and practices are rooted in this problematic lack of insight and understanding of the "inner nature," while this rarely means the same actors are either ignorant or inept in manipulating the symbols of commerce and social interaction.

Therefore, the essence of the matter is judging results by purposes and complete actions, not by apparent short-term "success." In the same way as ideologies affect judgement, unilateral thinking in practical matters inverts reality, and error appears to be "pragmatism," dissolution appears to be "normal," lack of direction appears to be "flexibility" and lack of meaning is exalted as "strategy."

I have limited this book to the problems around IT management and Information Security, to the errors caused by undue focus on one or the other aspect or modality of action and thought. It is nevertheless important to remember, when reading these pages, that my ultimate aim is not to just achieve balance among philosophical or cognitive paradigms, but to understand these and master them so that we are liberated from the unconscious laws that enslave our minds.

¹ <http://carlos-trigoso.com/public/negative-feedback-chain-in-solution-definition/>

² J.Forrester, 1968; Flood and Jackson, 1991

³ Theodore Roszak, "The Cult of Information," 1986

⁴ <http://carlos-trigoso.com/2011/04/04/what-security-shall-be/>

⁵ Jacques Lacan, "Encore" (Séminaire Livre XX), Paris 1975, p.32

⁶ Corporate and professional discourses orbit around the terms of "difference" (value as sign and status), "equivalence" (value as exchange/relation - market/commodity), "practicality" (value as use/object - utility/instrument), and "ambivalence" (value as symbol/gift).

⁷ Today "progress" just means cost and complexity reductions in the mind of the representatives of the absent master. Contrary to this, the "return" of ownership would mean increase of complexity and "cost" i.e. increased investment and organic transformation.

⁸ Donn Parker, "Beyond Risk Based Security," 2006

⁹ John Arnold, "Security Services Model," 2006

¹⁰ <https://collaboration.opengroup.org/jericho/presentations.htm>

¹¹ Wesley Newcomb Hohfeld (1879 – 1918)

-
- ¹² <http://carlos-trigoso.com/2011/04/04/what-security-shall-be/>
- ¹³ https://docs.google.com/document/edit?id=1IEVxIJesGn7h_vK1pa4yvjXY59ERtVqzn6yvX6mAlaM
- ¹⁴ <http://newschoolsecurity.com/2011/12/the-new-school-of-security-predictions/>
- ¹⁵ Ulises Mejias, <http://blog.ulisesmejias.com/2006/06/03/technology-without-ends-a-critique-of-technocracy-as-a-threat-to-being>
- ¹⁶ T.J. Rivers, 1993, quoted by U. Mejias
- ¹⁷ Theodore Roszak, "The Cult of Information," 1986
- ¹⁸ <http://shkaminski.com/Classes/Readings/Roszak.htm>
- ¹⁹ Walter Truett Anderson, http://articles.baltimoresun.com/1996-04-03/news/1996094015_1_ideology-political-parties-smart-machines
- ²⁰ Stephen Pepper, 1891-1972, <http://people.sunyit.edu/~harrell/Pepper/Index.htm>
- ²¹ Hayden White, 1928, <http://www.phillwebb.net/topics/History/White/White.htm>
- ²² <http://carlos-trigoso.com/2010/04/01/security-perspectives-protect-detect-direct-select/>
- ²³ Gareth Morgan, Gibson Burrell, "Sociological Paradigms and Organisational Analysis," 1979
- ²⁴ Herman Dooyeweerd, 1894-1977. See also: <http://www.dooy.salford.ac.uk/> and <http://www.members.shaw.ca/jgfriesen/Mainheadings/Dooyeweerd.html>
- ²⁵ R. Hirschheim, H.K. Klein, "Four paradigms of information systems development," 1989
- ²⁶ Stephen K. Moroney, "The Noetic Effects of Sin," 2000
- ²⁷ E. Brunner, "The Christian Doctrine of Creation and Redemption." See also: <http://www.asa3.org/ASA/topics/ethics/CSRSpring-1999-Moroney.html>

2. Freeing Security from “Risk Avoidance”

A Key Issue

A key issue for all organisations is the result or “value” gained from their investments.¹ This is especially relevant considering the large proportion of capital investments that go each year to information technologies.² In the 1980s researchers found evidence that information technologies offered competitive advantages to organisations,³ but some authors argued that IT benefits were difficult to measure, and that “Despite years of impressive technological improvements and investments there is not yet any evidence that information technology is improving productivity or any other measure of business performance.”⁴

According to Hannu Salmela⁵ studies on the relationship between IT investments and business performance could not show a positive relationship. Studies that are more recent show the same problem between IT investment and results.⁶ These reports coincide with what we, as IT and Security professionals, note in our work. We see low correlation between investment and organisational performance and in particular in the Security space, a tendency to constrain Security investment because organisations cannot find that correlation and prefer to mitigate or accept risks instead of addressing the problems in a comprehensive fashion.

There are some major differences between investments in IT security and ordinary investments. The main difference is that it is hard to decide the economic utility of Security.⁷ This is caused by the nature of the IT security measures. Investing in IT security or products usually will not provide direct returns in the sense of a measurable positive cash flow. If we take the conventional approach to Security, their main utility lies instead in reducing risks.

The second problem is that it is hard to determine the costs of IT in general and of Security solutions in particular. There are direct costs and indirect costs of any Security programme, and there are visible and invisible costs of the systems and processes that are replaced (or should be replaced) by any proposed Security solutions. It is equally hard to understand the financial justification to replace current processes.

The Security industry adopted early on the notion of Annual Loss Expectancy, to try to produce a financial argument for Security investments. ALE measures loss expectancy in terms of “single loss expectancy” multiplied by the “annual rate of occurrence” of a negative security event. This measure, still present in many Security manuals, is nevertheless difficult to use, and its output is not useful. This is because all ALE metrics need estimations for severity and probability of “loss events.” These, in turn, are not based on event frequencies but on expert estimates and recommendations. A key cause here is

that historical data of security events is very rarely published and is scarce even within organisations. In other words, Security based on risk estimations is hard because it is not objective.

Economic Concepts

As Security experts, we see that subjective approaches are unreliable, but many times, we apply these to fill in a “gap” in our methods. In the Security professional circles there is frequent criticism of the “lack of understanding” of “security measures” we find among business teams. This is erroneously classified as a “cultural” problem, as if non-security managers and specialists were by education or convention unable to understand our traditional approach.

Security professionals tend to distance themselves from the questionable and subjective methods around risk assessment by saying that, after all, the client is who identifies the risks and “we only provide the method.” I think that this is precisely the problem. Perception of risk is different at different organisational levels, and risk levels change depending on organisational changes and the actions of the different participants.

In fact, to a large extent, Security professionals are frustrated by the uncertain results of Security projects, but these have very little to do with risk calculations, and depend on correlations of forces, collaboration and contraposition of different levels and parts of the organisation. Our calculations may be correct, but the perceptions of risk, and the weights assigned to Security events are not objective at all.

Conventional risk analysis only shows how much the customer may “lose” under attack if all the conditions are known regarding the materialised security threat. This approach fails for a simple reason: any risk assessment changes the probabilities of the assumed Security events. Are Security experts considering the results of their own actions and those of their clients? Instead of continuing with the traditional approach, our work should assess and show how the business must change to be secure and compliant.

Economic and organizational ideas should be used systematically in the Security space. This is particularly difficult with working in the Public Sector; because economic concepts are absent from Security investment decisions. The notion of a return on investment becomes formal and loses meaning. This is a serious difficulty, but even in the Private Sector, most Security programmes are limited to the prevention of certain outcomes, and organisations do not calculate incident responses or remedial actions in economic terms. It becomes impossible to define a cost-benefit analysis.

Another challenge is how to determine what a security investment is due to the large variety of sub-areas and disciplines in our domains. For example, are Identity Management projects “Security investments”? For many organisations, Identity Management is not an area in Security but an operational or delivery aspect of IT in general.

This should lead us to open the discussion, and study Security and Identity Management in relation to organisational development and maturity. Technical experts tend to agree that it is an error to focus on

computing technologies knowing that risk management is not a technological problem; but surprisingly it is not equally easy to agree on the fact that a risk management focus—even one rooted in business considerations—is enough to develop a Security strategy. In this work I show how we can move away from a techno-centric direction and from a risk-based Security conception.

Don Parker made a fundamental contribution in this new direction in several articles and books.⁸

Parker writes: "There are too many interrelated unknown and known variables, with unknown values. They all change in unknown ways over time, depending on unknown future circumstances such as system and business changes, labour disputes, social and political changes, unknown enemies' failures and successes, and enemy and defender frailties and irrationalities. It is generally agreed there is inadequate loss experience data to support quantitative risk assessment applied to a specific instance, because of victims' needs for confidentiality. In addition, humans are notoriously bad at qualitative risk assessment. Finally, there is no proof of effectiveness or reported experience of performing security risk assessments cited in the security literature, because they are proprietary and confidential. "

I find these words by Parker —a recognised world authority in Information Security—should be enough motivation to explore to what extent the prevalent techno-centric risk-based methods are either fostering or halting better security practices. Let me underline that (the same as Parker) I do not think that we should abandon risk assessment methods, but that we must integrate these into a wider framework anchored on other Security perspectives.⁹

Decision Making

Martin Geddes described some years ago a pervasive problem in business decision making¹⁰: "I bet you've seen the following happen. There was an annual budget round, or some other big resource allocation decision. A guru from finance or strategic planning was tasked with producing the World's Most Complex Spreadsheet. Filled with tabs and links, it lists the options and the measurement criteria. Some criteria are hard numbers; some are softer issues that reasonable people could differ about. Each option is given a score for each criterion. That score could be its rank (inverted, to make the best one score highest). Or could just be a simple scale like 1-10. Or it could be some formulaic derivative of something like expected revenue. At the end, they all get combined by the formula from Hell (or just SUM), and a summary splurged into a PowerPoint deck.

"Then there is a Big Meeting. A number of exceedingly well-paid executives are called in to bless the result. But they do not like it. There is a big argument, and some 'adjustments' are made. Success in getting up the priority list is largely guided by force of personality and imaginative over-statement of expected project benefits. A few weeks later the senior VP of finance comes back from vacation, decides she does not like the outcome, and strikes out a project or two. In the meantime, a product development team keeps working on a project that did not make the cut, because the company has already invested so much in it, and you cannot kill the thing now. It is just work in progress, you know. The organization flounders in meeting its mission."

We in the Security arena have seen this happening so many times! To change this situation, Geddes suggests using the Analytic Hierarchy Process (AHP), first proposed by Thomas L. Saaty.¹¹ A NIST paper discussing AHP for Security Investment shows the application of this method to Security assessments.¹² The authors, still within a traditional approach, say that “the goal, Risk-Based Information System Security, appears at the top tier of the hierarchy,” while “the next lower level lists factors contributing to the goal, such as Confidentiality, Integrity, and Availability. These in turn serve as criteria for selecting among investment alternatives A, B, and C.”

The essence of AHP is the mathematical method used to aggregate numeric factors across the hierarchy. The authors correctly add: “This feature of being able to arrange the elements of a complex selection process into partial hierarchies and sub-hierarchies makes the AHP flexible and allows it to be tailored to an enterprise's level of investment management maturity.” Indeed, this is a good method leading to simultaneous evaluation of factors in a particular situation. We could easily adopt AHP for our normal, risk-based assessments, but this would only add a very sophisticated method on top of a weak foundation. How many reasons and influences should we select for the calculation?

As the NIST paper itself points out: “A low level of investment management maturity will require only a few criteria and sub-criteria to be ordered and evaluated with respect to an overall goal, whereas at a high level of investment management maturity there may be multiple levels, criteria, and sub-criteria.” How can we fit into this model the extraordinary complexity of investment management in global corporations?

So, let us keep in mind the direction suggested by Geddes and the value of the AHP method, but we need to develop a subdivision of the Security concerns based on principle, not on consensus or “committees of experts.” We may or may not use the AHP method itself, but its systemic approach is exemplary.

As I will show in later chapters of this book, my subdivision of the Security concerns into four paradigms or perspectives¹³ is a principled approach, by which the interaction of organisational and economic forces can be modelled and managed. The four Security perspectives are forces operating in any group or organisation, and must be studied and integrated, articulated and directed to ensure the completeness of our decision.

How are Decisions Made?

These thoughts lead to the realisation that the real problem is not how we demonstrate risk to the organisational actors, but how Security investment decisions are made with or without risk assessments or in spite of these. It is also vital to understand how risk assessments change the landscape that is being analysed. Ideally, our investigations should lead us to understand how Security is determined by the organisation itself. It is a guiding theory of this investigation the most important factor in any Security programme is the organisation, i.e. the structure and the dynamics of it.

Looking at this in an empirical way, the number of variables seems difficult to manage. The main source of uncertainty is organisation complexity itself, so we need to find a vantage point or a principle to reduce uncertainty and allow us to aggregate information.

There is much academic research about security investment decisions. In particular I note the work by G. Lawrence and M. Loeb,¹⁴ whose investment model paradoxically suggests investment required to protect an asset does not necessarily increase with the vulnerability of it. Loeb infers that protecting highly vulnerable information can be inordinately expensive and a firm may be acting rationally by concentrating investment on the protection of "mid-range vulnerabilities."

Beyond the puzzling appearance of this advice, we can recognise many of our own experiences, where the approach varies depending on the characteristics of the organisation, and how these classify their "mid-range vulnerabilities." In this sense Loeb's approach is meaningful but does not solve the problem and may serve as a justification for the current state of affairs in our profession.

If we take the experience of the Identity Management sub-discipline, we see that it has been positioned and "sold" as a tool, as a mechanism to gain savings in the user management cycle (by implementing password management for example).

Only a few years ago a new trend arose in our specialty, promoting role-based access control instead of service desk functions (like password management). This was a good trend and it showed the discipline was growing towards an extended strategy relying less on direct savings and more on organisational transformation.

The "service desk" strategy in some cases led to quick benefits as the reduction in incident calls and the cost of support personnel; but this focus minimises conscious, systemic business change. The result was Identity and Access Management remained as one more "tool" in the IT department, instead of becoming a pillar of enterprise security.

It is difficult to measure the economic contribution of Identity Management when it is constrained to service desk concerns. The business process engineering effort is not included in the calculations, and therefore the benefits obtained in service desk savings are often isolated, overvalued, and disconnected from other financial fundamentals.

For many experts, such a reduction of the Security and Identity sphere was comfortable, because it allowed them to avoid issues of organisational change. Sadly this also confined our discipline to the outskirts of Security, while this in turn remained on the margins of IT and enterprise-level thinking.

This type of adaptation was always associated with the refusal to address deeper questions that lie in the foundations of our profession. To progress from there, complex processes need to be addressed and new ideas are needed, in particular around the ideas of information and the "value of information." As we have seen, it is difficult to measure the value of Security investments and that seems to be widely accepted. There is no consensus though around the "value of information;" but

how could we measure the value saved or contributed by security if we do not have a clear concept of the object or subject we are protecting in the first place? What are we protecting?

There is a wide array of risk-taking propensities, from the entrepreneurial risk-taking, capitalist stances, to public sector, risk-avoiding positions. In all cases, the Security expert needs the concept of risk, both for those clients leaning towards risk-taking and for those taking a risk-avoidance stance. In other words, to be complete, risk management has to be a language both of risk-taking and risk-avoiding perspectives. Contrary to this, the dominant risk analysis disciplines do not reflect risk-taking propensities or business-like risk analysis, but quite a different stance where they try to "fundament" or justify security investment seeking only the avoidance of losses, and not business advantages in the market.

I see a series of results arising from this slant: risk-based security investment justifications are not positioning Security investment properly for normal risk-taking business operators and leaders. While these justifications are more acceptable for risk-avoiders in management and technical positions, Security investments end purely as expenses and therefore have to contend for resources with alternative IT expense items. The result is under-investment in Security across private and public sectors.

What we find in the market is that, in the whole, Security managers are frequently making sub-optimal or even wrong decisions. Following traditional schemas, the principle of "confidentiality" comes first, followed by "integrity" and "availability." This reflects the well-known Security "triad" or "CIA."¹⁵

Years ago, Donn Parker proposed a new model, the "Parkerian Hexad,"¹⁶ with the following classification:

- Confidentiality
- Possession or Control
- Integrity
- Authenticity
- Availability
- Utility

This expansion of the Security sub-areas is the right way to progress away from the initial limitations of our profession. Parker carefully distinguishes for example Confidentiality from Possession (Control), and Integrity from Authenticity. This leads to a better understanding of the real tasks of Security. Above all, we see that our goal is not only to "protect" certain objects, but also to ensure their validity (through Integrity and Utility, for example). The classical approach has no notion of Utility!

For Parker "Utility" means usefulness, including in particular data format and quality, and he remarks that Utility should not be confused with Availability. Is our profession ready to assimilate this conceptual expansion? Many years have passed since the proposal has been made with very little progress, but I think that we are now in a different situation, and the old models will be surpassed.

Risk and Probability Theory

Historically, the notion of risk has usually been defined in terms of loss and uncertainty. In classical decision theory the word “risk” describes a situation where both the possible “states of nature” and the “probabilities” associated with these states are known. In more recent times, risk is associated with unknown probabilities, mixing the sense of loss with the idea of uncertainty.

Real risk is frequently defined as the combination of chance and negative consequences in the real world. Different to this, perceived risk is defined as the estimate of “real risk” made without a theoretical model of the world. This dichotomy shows a very old tendency in Western rationalism by which perception and reality are separated. On the one hand, reality is assumed external to perception and on the other perception is taken as autonomous. This is the famous *Gegenstand*¹⁷ relation examined by H. Dooyeweerd,¹⁸ where the object of knowledge is separated from the process of knowledge in Western abstract thinking.

Risk and the perception of risk are one and the same “problem” or, better said, there is no risk outside of perception. Following this, there is a direct and complete argument against risk-based Security, using probability theory and standard Bayesian analysis.¹⁹

We need to start from the intrinsic duality of probability calculus²⁰: on the one hand, probability appears as based on frequencies of observations, on the other, as a judgment of authority or opinion. This duality exists since the beginning of Probability theory, and has never been resolved. In current Security methods, the frequency of observations and the authority of opinion are not clearly separated but mixed and confused.

If we apply Probability Theory to risk-based Security, we can see that our profession adopted the language of risk only superficially but did not extract all the effects of that move. In earlier sections we have seen how there was a tendency to speak about risk in terms of risk avoidance only, and now we can also understand why that is the case. A full adoption of Bayesian analysis would have led to a balanced view of risk and trust, i.e. risk and trust. A theory of trust is necessary to avoid the dead end of risk-based Security.

Now the goal is to demonstrate that while “risk management” is unilaterally defined around uncertainty and loss, “trust management” needs to be rooted in purpose and initiative. Instead of taking the existence of a trust boundary as an assumption, we start from the definition of the trust boundary (an act of risk-taking) as a precondition of a Security strategy.

Bayes' Rule

I started these reflections by stating there is no “Security theory.” There are many presuppositions, conceptual frameworks and principles, but these are accepted uncritically or even by default, unconsciously. As Security practitioners we have consensus knowledge but no science. This allows the existence and negative influence of what I have called many times the “techno-centric” approach.

In our professional practice, the most important unacknowledged influence is that of “decision theory,” in particular decision theory as practiced by neoclassical economics. This school, developed in the past century, takes the existence of rational behaviour as the basis of economics. When considering decisions under uncertainty, an individual is called “rational” when he or she behaves as a Bayesian decision-maker, making choices according to three principles:

- a) Defining uncertainty as a probability (if a fact is not known, the decision-maker relies on probabilistic beliefs)
- b) Capturing information by updating the “prior beliefs” according to the Bayes’ rule
- c) Following the “expected utility principle,” which states the choice should maximise the weighted average of probabilities and utilities

The conflation of economic behaviour with “rationality” is due to Leonard Savage²¹ and is called “subjective expected utility theory.” Savage’s goal was to reinforce the notion that to be “rational,” one had to be “economic,” in the sense of following economic rationality at an individual level.

I will not discuss here the problems of this approach or its validity (as this would need to address economic theory in itself). My point here is only that while economic theory may have a useable abstraction of the economic man, depicted as a “rational individual,” this by no means justifies utilizing this abstraction as a universal principle in other areas of knowledge, for example in organisation theory. In other words, I believe that organisational behaviour is only in part rational and/or individual. Even more importantly, individual rationality taken as the only principle of decision leads to a unilateral and destructive view of organisations of all types.

The rational-economic man is a successful abstraction in economic debate, if we judge success but the level of acceptance of neoclassical economics in academia and Government discourses since the 1980s. Nevertheless, the debate is more than open regarding the complete lack of success of this school in terms of economic development and income distribution in the countries that accepted this “rationality” as political goal.

Now, this global success of neoclassical economics and the theory of the “rational man” also influenced Business Management theories and, indirectly, all professions around information technologies. On the one hand this influence has been positive, linking the IT specialties to wider cultural and academic debates, but, because neoclassical economics was accepted uncritically, its principles became intertwined with existing pre-conceptions and ideologies. The notions around subjective probability and Bayesian statistics were transmuted into justifications for risk-based Security practices.

Let us review quickly what Bayesianism is about.²² For two events A and B, with probabilities $p(A)$ and $p(B)$, and assuming that $p(B), p(A)$ –that is the joint probability– not equal to zero, the definition of Bayesian conditional probability of A when B is given is stated by the formula $p(A|B) = p(A \& B) / p(B)$.

$A \& B$ here denotes the case where both A and B occur and $p(A \& B)$ denotes that event's probability; while $p(A | B)$ is the probability that event A will occur given the fact that B has already occurred.

Bayes' rule is a way of converting a probability (e.g. $p(A|B)$) into a probability $p(B|A)$. This means transforming the probability that A occurs given that B has occurred, to the probability that B occurs when A is given.

Bayesian theory is very well-established and is a major tool of scientific research and decision-making, but these principles are not used uniformly across all disciplines, and in particular they are used in a wrong way in some areas of business management, including IT and Security. The confusion centres on how the concept of "objective probability" is used within research to build decision scenarios. In the Security space, this refers to the use of "risk factors" for decision-making.

A major error consists in the arbitrary transfer of catalogued "risk factors" (which often are not objective but consensual or expert-driven) to risk assessments in particular cases. Instead of applying a different probability model for each specific case, the risk factor weightings are carried over to concrete assessments. The problem is that in concrete cases, only a subjective analysis is possible, based on correlation of judgments and risk models within the situation.

What this means is the Bayesian principle is misapplied and misunderstood. This also means that we should call subjective what is subjective, and not pretend there are any objective threat frequencies or scientific risk models. The problem does not stop there, because expert models have some value after all. The problem actually begins when the supposed expert risk model or consensual threat landscape blocks the development of an internal and subjective (Bayesian) risk analysis.

Out of all the methodologies that have appeared to elicit proper organisational security the best in my opinion is Carnegie Mellon's Octave (<http://www.cert.org/octave/>). This is so because of the emphasis on organisational debriefing and input, versus undue emphasis on given or assumed threat scenarios.

Risk analysis is always subjective even when we use an "objective" Bayesian method, i.e. when we use frequency data as prior probabilities. There is no past risk, because risk is derived from conscious action (decision). This means the decisions and perspectives of all the actors in a particular situation determine directly and indirectly the actual risk and trust landscape. A consequence of this is that we can see now the most important error of risk-based Security is double: First, it is not based on objective measurements, but only subjective or consensual threat catalogues. Second, when it should proceed to analyse and consolidate subjective probability (i.e. at the level of organisational management) it does not do so, because it has already substituted the "given," expert-derived probabilities for real ones.

Security as Insurance

In an often-referenced paper, Kevin Soo Hoo²³ addresses the problems of risk-based Security and indirectly points to the errors in probability theory. Donn Parker considers this paper as "the most complete mathematical model of risk assessment methods ever developed."²⁴

K. Soo Hoo's work shows that, while trying to overcome the issues created by risk-based security, he proposes risk-based insurance for information assets. Parker probably did not think much of this change in emphasis, but I believe that it is very useful for Security practitioners still attached to the old methods.²⁵

Soo Hoo writes: "In retrospect, three fatal flaws doomed the common framework and its ALE-based brethren to failure. The deficiencies are as much a reflection of the inventors' biases as they are an illustration of the challenges that face any attempt to model computer security risks. First, the methodology's scenario-generation mechanism created an assessment task of infeasible proportions. In any mathematical or computer modelling endeavour, a balance must be struck between model simplicity and faithful replication of the modelled system. If the model errs on the side of simplicity, then it may not be sufficiently accurate to be of any use. If, on the other hand, it errs on the side of faithful replication, then its implementation may be so overwhelming as to render it impracticable. This tension pervades every modelling effort. Unfortunately, the ALE-based methodologies tended to favour significantly greater detail than was efficiently feasible to describe."²⁶

Contrary to this, Soo Hoo proposes a successive-recursive approach on the lines suggested by the US National Research Council: "an analytic-deliberative process . . . [whose] success depends critically on systematic analysis that is appropriate to the problem, responds to the needs of the interested and affected parties, and treats uncertainties of importance to the decision problem in a comprehensible way. Success also depends on deliberations that formulate the decision problem, guide analysis to improve decision participants' understanding, seek the meaning of analytic findings and uncertainties, and improve the ability of interested and affected parties to participate effectively in the risk decision process."²⁷

An example of the wrong approaches criticised by Soo Hoo is the Factor Analysis of Information Risk (FAIR).²⁸ This model is valued by some Security experts as a better alternative to traditional risk assessments, but I find it seriously affected by wrong notions of probability and risk.

As indicated before, traditional risk assessment requires determining the likelihood of future harm involving specific information to be protected. In the great majority of cases this determination cannot be made internally to the organisation because there is insufficient loss experience in the specific circumstances being assessed, so the Security experts import some consensual model and substitute it for real Bayesian analysis. Risk assessment also would require estimations of future loss from each type of incident, but the value of the information involved is often not material and hard to determine. Frequency data and loss sizes must be combined in a logical way to get any results, but the quality of the data is poor.²⁹

As Parker indicates, the last step mentioned above requires "selecting controls," but risk assessments only recognise "how much could be lost," not what kind of controls are necessary and much less what kind of technologies are optimal. Any controls have to be selected by a different set of experts in many cases, or through different methods and additional risk assessments to see if the controls work at all.

More critically, the traditional approach does not take into account the change in the risk and trust landscape because of the risk assessment itself. This reveals the lack of proper probability theory concepts and mixes up objective with subjective Bayesian measures.

The FAIR model is also trapped in a series of confusions, for example when the authors describe risk as "the probable frequency and probable magnitude of future loss." Here risk becomes a probability of frequency multiplied by a probability of magnitude of loss; i.e. a derived probability or a probability of a probability. The authors insist that "risk is a probability issue" and that "risk has both a frequency and a magnitude component." The problem with all of this is the implied nature of risk, where decision and action are completely lost. Risk becomes once more a matter of classification of expectations in some standardised framework.

The confusion is notorious when the FAIR proponents write their risk definition "applies equally well regardless of whether we are talking about investment, market, credit, legal, insurance or any of the other risk domains including information risk," and that "the fundamental nature of risk is universal, regardless of context." What does "regardless of context" mean? What remains of Bayesian analysis here if the context becomes irrelevant? Are we talking about objective probabilities, given frequencies of events that are already classified in the FAIR framework? Certainly not, as the FAIR model is also a mechanism to collate subjective valuations. Do loss and magnitude of loss event probability pre-exist to risk assessments? I believe the FAIR team have not asked themselves this question, or the more important one: Do threat and risk landscapes change with risk assessments?

I believe that Soo Hoo tried to shift the debate by abandoning risk-based security and suggesting an alternative to justify IT Security initiatives. He settled on a type of "insurance," based on market pricing of risk coverage. In spite of the good argumentation in Soo Hoo's paper, this is only a partial answer to the problems we are discussing. Security insurance may be a complement but not a substitute to Security strategy and policy. On the positive side, Soo Hoo's paper points to the essential conflict between an inherited "expert" threat model and the internally developed model based on "the needs of the affected parties." This is also my aim, through the application of the Security Perspectives model; i.e. the contra-posed and correlated Security paradigms that have to be elicited and grasped through an analytic-deliberative process.

Luhmann on Trust

The whole direction of risk-based security is flawed in that it ignores both well-established probability theory and basic principles of organisational analysis. It is essential to bring into this discussion the idea that risk needs a decision-maker, and that risk implies trust.

Niklas Luhmann, the German sociologist, studied these problems and arrived at very valuable ideas that should be part of the Security discipline. He wrote "[Trust] depends not on inherent danger but on risk. Risks, however, emerge only as a component of decision and action. They do not exist by themselves. If you refrain from action you run no risk. It is a purely internal calculation of external conditions, which creates risk. Although it may be obvious that it is worthwhile, or even unavoidable,

to embark on a risky course - seeing a doctor, for instance, instead of suffering alone - it nevertheless remains one's own choice, or so it seems if a situation is defined as a situation of trust.

“In other words, trust is based on a circular relation between risk and action, both being complementary requirements. Action defines itself in relation to a particular risk as external (future) possibility, although risk at the same time is inherent in action and exists only if the actor chooses to incur the chance of unfortunate consequences and to trust. Risk is at once in and out of action: it is a way action refers to itself, a paradoxical way of conceiving action, and it may be appropriate to say that just as symbols represent a re-entry of the difference between familiar and unfamiliar into the familiar, so too risk represents a re-entry of the difference between controllable and uncontrollable into the controllable.

“Whether one places trust in future events, the perception, and evaluation of risk is a highly subjective matter. It differentiates people and promotes a different type of risk-seeking or risk-avoiding, trusting or distrusting, individuality. [...]”³⁰

I will take this line of thought further when correlating risk and trust in our practice, and the four perspectives of Security.

While FAIR and other frameworks and ontologies strive to "approach" the way economics understands risk, they fail due to uncritical and poor adoption of probability theory. The objective is confused with the subjective, and risk managers end up blocking real risk and trust modelling.

A correct understanding of risk implies that either in private or public sectors, the decision-maker, while defining a trust boundary, simultaneously takes risk, and accepts a risk level. Risk is neither purely objective nor purely subjective but objective and subjective at the same time. Decisions and actions, for example investment decisions, entail uncertainty about the outcomes and change the risk landscape during their inception. Therefore, the Security professional needs to grasp the business model of the organisation (the trust boundary) and the associated risk involved in it, overcoming the slant towards “protection” of assets. Valuable informational assets do not exist outside of the definition of the business model and the risk-trust correlation that arises from it.

In this way Security analysis becomes a proper micro-economic discipline and finally “aligns” with business.

Identity Management Beyond the Standard Approach

Identity Management, as a discipline or domain within IT Security, is also in need of “alignment.” To achieve this, my proposal is that we put the principles of Identity Data Management and Identity Data Ownership at the centre of attention. Contrary to appearances and technological trends, Identity Management is essentially data management and not a “tool” in operational security. A correct understanding will lead to the application of both economic and industry standards in the sphere of information management.

Among the Security disciplines, Identity Management is the most affected by organisational factors, and the one that impacts more organisational processes and structures. These ideas run against a major obstacle, which I call the traditional or “standard” approach to Security.

The starting point of the “standard approach” is identifying the enterprise “informational assets.” Later, these assets are assessed to estimate their “value” and the potential threats they are exposed to. This approach has its historical origins in the protection of business data repositories and central computing facilities and networks. The standard approach then proceeds to determine the level of risk, which is positioned as a “quantitative measure.” In the standard approach, there is no other way to address security and, thus, no other way to propose, design and operate security services.

My thesis is that Identity Management cannot be fruitfully approached in this way. In general, less than a quarter of the drivers and requirements for Identity Management can be associated with the notion of informational risk or even with informational “assets.” On the other hand, only a small part of investment requirements and decisions in this area can be determined by risk calculations.³¹ To move beyond these limitations, Identity Management needs to gain a balanced focus encompassing four areas: Direction, Selection, Protection, and Verification.³²

A similar correlation of perspectives could be applied to all security disciplines and not only to Identity Management, but it is nevertheless the case that this domain is more negatively affected by the “standard approach” than any other Security discipline. All Security disciplines should be rooted in the “Circle of Trust” (as explained in my previous work³³): Trust is first defined, then it is established, then it is enforced, then--finally--it is verified. The circle of trust can thus be readily mapped to the areas of Direction, Selection, Protection, and Verification, in that order.

In the traditional or standard approach, Security is overwhelmingly associated with the perspective of Protection and secondarily with Verification disciplines, so we need to work towards an integrated view comprising four fundamental and complementary perspectives:

- It is essential to understand there is no “security” without Direction (Governance), especially not without the definition of what the organization wants to preserve as a level and boundary of trust. The organization's policies ownership structure comes first, and the definition of what is a trusted environment is a precondition for all the other perspectives.
- The disciplines of Protection, mostly centred on network, platform and application security have been historically the “home” of our profession, but now a well-established trend to go beyond perimeter and zone protection is changing this.³⁴
- In the past few years, accelerated by increasing regulatory pressure, the area of Verification (Compliance) has come to a second place in importance after Protection. It is evident there can be no Compliance without Protection and Direction.
- Finally, even more recently in history, still immature, comes the perspective of Selection. It has grown out of the Protection quadrant, where it stayed as simple “access controls” and includes now role management, provisioning and authorisation workflows.

Overall, then, Identity Management sub-processes appear as natural components of the Security disciplines and their expansion across the enterprise. This also reflects increasing linkage with business and organisational concerns. While the initial layers of security solutions were mostly technical the more recent are business-based and cannot exist without business process changes as indicated in other parts of this work. All of this has important consequences for security architecture and investment decisions.

For many years, Security architecture and investment decisions have been dominated by preference for the Protection disciplines. Building up the perimeter and guaranteeing security zones was generally equated to “securing the environment.” The Protection disciplines still form today the strongest area in any organisation in quantitative terms. This period has left a mark in the decision process. Decisions are led by a preference for risk-based or threat-vulnerability analyses.

The situation has evolved with emerging Verification and Compliance concerns. But this has not changed the fundamental idea of "asset protection" and "perimeter security."

Nothing of the above denies the problems of Compliance and Vulnerability to external or internal attack, but I think that it can be demonstrated the Protection and risk-based approach effectively ignores important parts of business economics precisely because of its focus on a limited idea of risk (analysed in the previous section). On closer analysis, the traditional approach reveals its lack of a notion of business growth. Whereas in the business world investment is fundamentally done under the combined notions of investment risk and opportunity, in the Information Security world and in particular in Identity Management we are still working under the static and defensive notion of asset protection.

So, in conclusion, to present the whole case of Security, and of Identity Management in particular, it is essential to include those opportunities and benefits that can be derived from transformation and process efficiencies and are complementary to the other areas of security. For this reason I will explain in later sections how to overcome the standard approach by furthering the ideas of Identity Data Management and Identity Data Ownership.

Trust and Respect

Hans Wierenga recently published in SOA Magazine (Issue XLII, August 2010) a brilliant article³⁵ analysing the predicament of the Security disciplines. Wierenga writes:

“Unfortunately, the current information security vocabulary--in particular, as embodied in standards such as the ISO 27000 family of standards, CRAMM and COBIT--- is structurally and fundamentally unsuitable for expressing the information security requirements of the 21st century. The key terms of this vocabulary are confidentiality, integrity, and availability, better known under the acronym CIA. As we shall show in this article, there are many, many goals which are not adequately covered by these terms, nevertheless must be achieved in order for an organisation to have good information security in the Internet age.”

“However, the vocabulary is not the only problem with CIA: the way that it is applied is also inadequate. CIA is applied to the individual information assets of organisations, with little regard for the collective impact these assets have on the experiences of customers, suppliers, and employees. But it is this collective impact that determines the business value of information security. In other words, the security consultancy industry standards do not just employ the wrong words, but they also apply them to the wrong things. The CIA paradigm entirely ignores the fact the whole is more than the sum of the parts, blithely assuming that if each individual information system is secure the whole is too. This way of thinking is hardwired into the standard approach of the information security consultancy industry, which involves making an inventory of the information systems and then working out how to make each of them secure.”

In previous sections of this work I classified the standard Information Security approach as technocentric or mechanistic, and explained how it is linked to the idea that information is an object that needs “protection.” In later sections I will explain how the machine metaphor leads to an idea of information as an object or physical substance. Wierenga does not employ a metaphor analysis or world-view approach, but he clearly sees the problems with the standard thinking arising from a specific ideology:

“If all the money ever invested in implementing CIA [confidentiality, integrity, availability] was one giant waste, it wouldn't matter because there is no way to tell. We may know the result of this investment, but not what the result would have been without it. Using words that do not adequately express the goals we wish to achieve, applying an approach that considers only the parts but not the whole, and not measuring how effective you are is a recipe for ineffective solutions. That need not be a problem if the whole point of the exercise is to enable those responsible to claim they took the best advice and did everything they could, but not everybody can afford to take such a position. In this paper we shall discuss how the conventional wisdom of the information security consultancy industry can be improved upon in order to deliver measurable business value. We shall introduce more fitting terms, which enable us to maximise this business value, and we shall introduce an approach that goes from the whole to the parts. The new terms - trust, respect and utility - enable us to focus on the business value of information security and lead to better information security solutions. We shall show how engendering trust, showing respect, and delivering utility change the information security landscape. We shall demonstrate how they improve on the CIA-goals and approach, and discuss whether it makes sense to incorporate the old wisdom into the new.”

On the basis of this approach, Wierenga proposes new guiding principles for Information Security -- Trust, Respect and Utility-- and further expands Trust with principles to “Create Transparency, Right Wrongs, Confront Reality, Clarify Expectations, Practice Accountability, and Keep Commitments.” Central to Wierenga’s thinking is the principle of Trust, which should be at the centre of Information Security. This is also essential to my approach to Information Security and Identity Management as the reader must have seen in previous sections.

With similar aims as those of Donn Parker and Hans Wierenga, I am proposing a replacement, not a variation of the standard CIA “triad,” by using the concepts of Direction, Selection, Protection, and Verification.³⁶ There is a potential mapping of this new model to the CIA triad, if we assume that Confidentiality roughly is reflected in the Selection perspective, Integrity may be seen in some cases as represented in Verification, and Availability in Protection, but this mapping is not satisfactory. On the other hand, the CIA triad misses the notions of Direction (or Governance).

The perspective of Direction reflects all those factors that escape the techno-centric or traditional approach. In particular, it is important to note the disciplines of Direction encompass definition of trust, assurance, intent, decision, and business model. The four-sided model does not make claims of complete originality. As I stated in a previous section, it is based on work by John Arnold and other Security thinkers, especially Donn Parker³⁷ and Hans Wierenga.³⁸

Wierenga understands that a deep change in Information Security needs a new vision: “A new approach to information security is hardly possible without a new way of looking at information systems. In this paper we shall apply the service-oriented architecture paradigm for that purpose. The paradigm describes all interactions in terms of services, in which a requestor asks an agent for something to be done, and the agent ensures that it gets done and delivers a response to the requestor. This way of thinking can be applied at a business level, to describe interactions between organisations, at a functional level, to describe how the activities of which business processes are comprised interact, and at the level of information systems, in order to describe how systems and parts of systems interact. Applying it at all levels enables an organisation to make the connection between each and every part of its information processing and the business value that it delivers.”

Wierenga develops his work around the ideas and methods of Service Oriented Architecture (SOA), an effort that is rarely seen in the Security disciplines, often characterised by “point solutions” and remedial work. Thinking that SOA is something irrelevant now, either because of the Cloud or other perceived problems, would be seriously misinformed. I will show now the new period of Security in and for the Cloud, and constitute the natural and logical progression of SOA at a global level.

¹ Hannu Salmela, “Dynamic and emergent information systems strategy formulation and implementation,” 2002

² Hannu Salmela, “Assessing the Business Consequences of Systems Risk,” 2003

³ Porter and Millar, 1985; Parsons, 1983; McFarlan 1984

⁴ Brynjolfsson, 1993

⁵ Salmela, 1997

⁶ Whiting, 1996; Pervan, 1998

⁷ Ross Anderson, “Why Information Security is Hard,” 2001 <http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf>

⁸ See especially: Donn B. Parker, “Risks of Risk-Based Security,” Communications of the ACM, March 2007

⁹ Jeff Lowder, attempting to defend risk-based security, gives reason to Donn Parker: “Parker's third supporting argument may be categorised as a “lack of evidence” argument. According to Parker, there is no study that demonstrates that security risk management actually works. In his words, “No study has ever been published to demonstrate the validity of information security risk assessment, measurement and control based on real experience.” I agree with Parker's implicit assumption that we should require evidence that information security RA works. And I suspect that Parker is probably

correct that there has been no study published that demonstrates the validity of ISRA [information security risk analysis] specifically. By itself, however, that fact hardly calls into question the validity of the ISRA discipline. There also has been no empirical study published that demonstrates the invalidity of ISRA." See: J. Lowder, ISSA Journal, December 2010. Lowder is on very shaky ground here, especially because of his assumption that the probability of attack can be estimated for a particular organisation based on the beliefs of the expert community even if the evidence is not known. This would mean that risk and risk reduction are "measurable" purely relying on a subjective variant of Bayesian analysis.

¹⁰ M.Geddes, "Expert Choices," 2004, <http://www.telepocalypse.net/archives/000224.html>

¹¹ T.L. Saaty, "The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation," 1980

¹² B. C. Lippiatt and S. K. Fuller, "An Analytical Approach to Cost-Effective, Risk-Based Budgeting for Federal Information System Security," 2007, http://www.bfml.nist.gov/oe/publications/nistirs/NISTIR_7385.pdf

¹³ <http://carlos-trigoso.com/public/security-perspectives-2012/>

¹⁴ Gordon, Lawrence A. and Martin P. Loeb, "Return on Information Security Investments: Myths vs. Reality," Strategic Finance, November 2002

¹⁵ Information Security Handbook, 1997, <http://www.cccure.org/Documents/HISM/ewtoc.html>

¹⁶ Donn B. Parker, "Fighting Computer Crime," 1998

¹⁷ "Object" in German

¹⁸ See Glenn Friesen's treatment of this problem here:

<http://www.members.shaw.ca/jgfriesen/Mainheadings/Epistemology1.html>

¹⁹ For an introductory text see J. M. Bernardo's "Reference Analysis," <http://www.uv.es/~bernardo/RefAna.pdf>

²⁰ Ian Hacking, "The Emergence of Probability," 2006

²¹ Leonard J. Savage, "The foundations of Statistics," 1954)

²² Probability calculus approach due to Thomas Bayes, 1701 – 1761, English mathematician

²³ Kevin Soo Hoo, "How Much Is Enough? A Risk-Management Approach to Computer Security," 2000

²⁴ Donn B. Parker, "Making The Case For Replacing Risk Based Security," The ISSA Journal, 2006

²⁵ Soo Hoo cites a 1996 study titled "Vulnerability Analysis and Assessment Program Results," to note that out of a total of 38,000 security breach attempts, 24,700 or 65% were successful, 988 or 2.6% were detected, and only 267 or 0.7% were reported. Security breaches underreporting is still pervasive across the world, but there are strong initiatives by governments to make breach reporting obligatory. In any case, the proportions noted here still a good approximation according to my own experience. Lack of effective security breach statistics is a severe obstacle for the assumed "objectivity" of risk-based security. Soo Hoo writes: "In July 1996, the agency [Defense Information Systems Agency (DISA)] issued its one and only publicly distributed report on this ongoing program's results. The report estimated that 96 percent of the successful break-ins were undetected, and, of the few that were detected, only 27 percent were reported [...]."

²⁶ Kevin Soo Hoo, "How Much Is Enough? A Risk-Management Approach to Computer Security," 2000, page 7

²⁷ National Research Council, Committee on Risk Characterization, "Understanding Risk: Information Decisions in a Democratic Society," National Academy Press, 1996

²⁸ FAIR is a model proposed by the Risk Management Insight group. See:

http://riskmanagementinsight.com/media/docs/FAIR_brag.pdf

²⁹ To address these problems D. Parker proposes a "due care approach" in "Fighting Computer Crime: a new framework for protecting information," 1998

³⁰ N. Luhmann, "Familiarity, Confidence, Trust: Problems and Alternatives," 2000

http://onemvweb.com/sources/sources/familiarity_confidence_trust.pdf

³¹ Identity Management projects should be assessed in terms of indirect and direct financial benefits and costs, as well as indirect and direct operational risks and opportunities.

³² <http://carlos-trigoso.com/public/four-perspectives-on-risk-and-trust/>

³³ <http://carlos-trigoso.com/2010/08/15/iam-in-the-circle-of-trust/>

³⁴ The most advanced views on this can be found in the Jericho Forum website.

<https://collaboration.opengroup.org/jericho/publications.htm>

³⁵ Hans Wierenga, "Why the Information Security Consultancy Industry Needs a Major Overhaul," 2010

<http://www.soamag.com/l42/0810-1.php>

³⁶ See: <http://carlos-trigoso.com/mind-maps/security-perspectives/>

³⁷ See also: <http://www.computersecurityhandbook.com/author-parker.html>

³⁸ See: <http://www.infoq.com/articles/10-soa-commandments>

3. Security and Information: Access Management

Dependency of Information Security

In our study of Information Security and Identity Management the most important idea should be “information,” not “security.” Security is the predicate of information: we say that information is “secure,” not that we practice some security “for” information. Now, what is “information”? In this period of dominant techno-centrism, the notion of information seems self-evident and beyond doubt, and Security professionals never discuss what is meant by it. We concentrate on what security could mean, but not on what we are “securing.” Because of that presupposition, our entire worldview becomes weak and degenerates into a series of “keywords” and simplifications.¹

Here is a text from the standard CISSP CBK book: “Information security practices protect the assets of the organisation through carrying out managerial, technical, and operational controls. Information assets must be managed correctly to lessen the risk of financial loss — just as financial assets are managed through finance departments and human assets (people) are managed and cared for by the human resources department and associated code of conduct and employment policies and practices. Failure to protect the information assets from loss, destruction, or unexpected alteration can result in significant losses of productivity, reputation, or finances. Information is an asset that must be protected, as well as the software and hardware, which support the storage and retrieval of the information.”² This condenses everything I need to comment on about traditional approaches to Security.

We seem content with elementary definitions like these, focused on the idea of “safe-guarding” an organisation's data from unauthorised access or change; and we also take as a definitive truth that organisations have “informational assets,” presuming that we know exactly what these are.³ Once the definition is given –and this happens in almost all manuals, textbooks and documents about Information Security-- the terms are rarely discussed in depth.

The most important task in this period is therefore to examine and fully determine what information is, and what role it has in society, economics, business, and professional practices. We then need to have an understanding of what informational assets are, and finally what it means to “secure” them. Only then can we start speaking about IT Management and Security on a solid foundation.

Any direction or proposal for IT and Security management needs to consider these domains are enclosed within a wider sphere. IT and Information Security are dependent areas of business operations. Business management itself is dependent on the surrounding social and economic structures and practices. Therefore, any try to resolve problems in the limited context of IT will fail if it does not express a real business, economic and social context.

IT and Security management need a philosophical stance, a search for principles and truth that may anchor better future solutions. Considering this need, though, it is difficult to be optimistic in the face of the permanent anti-philosophical stance of the technical professions. The IT specialities and Security are not accustomed to this, even despite the permanent flow of sub-optimal and failed goals and technologies that we see every day. This anti-philosophical stance reveals itself in the illusion of technical progress and the assumption that all technical progress is good. It is also visible in the pervasive lack of knowledge of the problematic of Information Theory and the role of information in society.

To do philosophy is, largely, to think with abstractions. Technical professionals or specialists close to the technical areas dislike “abstractions” and seem prefer “concrete” or practical matters. There is a great confusion in this rejection of the abstract. In fact, thought is impossible without abstractions, and the mere act of assuming or accepting some principles is already a major abstraction underlying what we commonly think as Information Security.

As mentioned above, Security professionals take for granted what information is and take it more or less as a given object or “value” existing “inside” of organisations, an object of value that needs to be “protected” against unauthorised access. Here you see already abstractions at play: the terms around information, for example the “value” of information, are abstract presuppositions, not concrete or practical at all, but instead an inherited, socially conditioned abstraction.

This presupposition sits like a background or a curtain behind everything we discuss when we talk about security. A background so opaque and extended that we do not even see it is there. It is an abstraction in the most common sense of the word.

So involuntarily, when refusing to discuss Information Theory or other areas that might clarify the context of our profession, when expressing preference for “practical things” we are giving in to inherited, given, ideological abstractions, and we do so uncritically and passively.

My work follows a different path, a philosophical path, starting with the analysis of presuppositions and worldviews. Ideas are produced by analysis and synthesis, aggregation and inference, analogy and selection of explanations that fit the evidence. Philosophy has a bad name in the techno-centric professions, but is nothing else but the science of thinking and it has a rigorous practice. Philosophy needs a desire to search deeper, beyond consensual knowledge because, after all, accepted truths are what determine our current predicaments, what has brought us to where we are now.

Four Classes of Access Control

A good starting point for this journey is analysing the notion of Access Management, an everyday idea used by Security experts. We think we know what this means, what we are talking about, when we present our solutions for “user access control.” We are so used to this idea that we don’t stop to consider how it is constructed, what parts it has, what variations it admits; but, if we had an idea of the

complex ramifications of access management, we could start building or rebuilding a Security theory around this foundation.⁴

A first analysis shows there are four classes of access controls:

- Granting access to resources: by allowing users or their tools to access data sets or data stores.
- Limiting access to resources, to ensure a user (or his/her tools) do not do more than they are authorised to do.
- Preventing access to resources, to ensure that users do not damage these or access information intended for others.
- Terminating access to resources: by removing access rights from users or their tools when these are not authorised or lose authorisation to access data sets or data stores.

When considering these forms, we immediately see an application of the four elementary perspectives mentioned in previous sections:

- Granting access corresponds to “direction” disciplines, i.e. activities around trust definition.
- Limiting access corresponds to “selection” disciplines, i.e. activities around trust allocation.
- Preventing access corresponds to “protection” disciplines, i.e. activities around trust enforcement.
- Terminating access corresponds to “verification” disciplines (compliance); i.e. activities around detection and validation of user access.

So here, we have a first analysis of Access Management. I believe that this analysis cannot be disputed and is self-evident for all Security specialists. Nevertheless, this approach, simple as it seems, immediately takes us beyond the traditional or standard “Protection” approach. From the side of the modalities of access control, we have various activities that are far more complete and complex than reducing security to access and access to mere protection.

The second level of abstraction should be to identify and reveal the object of access controls. Although we in the Security arena talk every day about access controls, we rarely discuss what we are protecting. Some colleagues dismiss any discussion, saying it is obvious we are “protecting information.” With that, the discussion is declared finished. In my experience, when the Security practitioner reaches that point, he or she feels self-justified as being “pragmatic.” Everybody seems to “know” the object of our protection efforts. Information, within the techno-centric view, appears as an object, a material substance that can be encased, covered, stored, and manipulated as a thing.

This ideological thinking and presupposition is especially visible among technology vendors, where the ideology also becomes part of the commercial positioning effort. Some companies make this plain when identifying as “suppliers of information security” or even “specialists in information.” These discourses take for granted that the audience, perhaps company executives or advisers, will automatically agree with shared notions of what Information is, and what this means for Information Security.

Not all technologists, consultants, or vendors are impervious to theoretical thinking, and some will remember research or academic results when pressed for a deeper view of these matters. For example, people will remember the ISO 27001 or the CISSP Common Body of Knowledge training, and maintain there is after all a Security Theory based on “security models.”⁵

That is true: a small set of security models exists, none of which is a theory, but a more or less complete set of logical statements focused on user access controls, for example Bell-La Padula,⁶ Biba,⁷ Discretionary Access Control,⁸ Clark-Wilson⁹ and Non-Interference.¹⁰ All these models are based on ideas around the nature of information and the notion of “information flow.” So for example, these models abstract human actions for reading or writing¹¹ data from or into information stores. A presupposition of all these models is a concept of information, where it is reduced to a material form or storage of written signals. One of these models, Nondeducibility theory,¹² is particularly interesting, because it is clearly based on information theory and the notion of “information flow.” This model assumes *that information flows* in a system between “high-level objects” and “low-level objects.”¹³ In this framework, there are several interpretations possible, as analysed by John MacLean,¹⁴ for example, a Security policy could allow for information flow from low-level objects towards high-level objects. This is not so relevant here, as I want to focus on the use of the “flow of information” idea. Either in the earlier notions of writing and reading, or in the ideas of information sharing or flowing, what is clearly at play is a notion of information as a substance, that somehow moves from one entity to another. This conception is very much at the base of all our Security models.

Intuitively and in common discourse, we assume the “reality” of information as a substance with properties similar to water or air, that is, a substance that moves and flows between containers or other objects, “passing” from one to the other. When information “flows” for example from a protected envelope to a lesser protected one, we interpret this as a “data leak.”

This is realistic enough, and perhaps such a definition of data leak may be enough to give base to a “security policy.” Nevertheless, in any organisation, Security practices are in fact impossible to reduce to the models that we have inherited and all “security principles” we know. In reality, the most clever logical access morel (write, read, deduce, etc.) can only represent a small fragment of an organisation’s Security practices, as we have always a combination of levels, sometimes dozens of variations of these models are needed to manage documents and data in all possible situations.

As organisations evolve, even military ones have to adopt and combine several Security models and leave behind uniform mechanisms for access control. More so, this happens in the private sector, where it is normal to find different “models” for different divisions, and even within divisions and application types. The trend goes even beyond that, as we are seeing different user types covered by the same “model” as well as different models for the same user type, i.e. for the same security classification for users.

This situation shows that when looking into the well-known “security models” cited above, we are not in front of Security Theories, but only fragmentary formulations for very specific cases, some of which

were perhaps suitable when computers usage was rare and limited to bureaucratic organisations. So where do we stand now? What is Access Management in this new situation?

Access and Indirection, Secrecy and Authenticity

Another aspect these models have in common, besides a similar notion of information as an object and security as encasement or “protection,” is that all of them equate Security with “secrecy.” It is not strange they do so, as many of the models were developed during the introduction of electronic computing into military and public agencies.

Under those circumstances, “user access” had to be considered as an event that potentially represented a threat for secrecy and control. In other words, user access is conceived in terms of enforcement of access permissions or “access control lists.” This reductionist approach was enough in a period where users had what can be termed “direct” access to a resource, for example, directly typing their user names into a login screen and reading information off the screen itself; although even in those cases information access was never direct. A notion of access inherited from printed or written materials, held in folders or cabinets, behind doors, was expeditiously imposed on a different environment consisting on electronic computers and binary media.

Up to some point, this new abstraction—seeing electronic devices and media as paper and cabinets—does work when routes of access are direct, as indicated above. This maintains the illusion of a person either being authorised or not to “see” some information or to “write” data into the repository he or she is accessing. In reality, since the beginning of electronic computing, access is indirect, and the whole evolution of these technologies led to increasing indirection, remoteness, and mediation of access. We could summarise what has happened by saying that access is always indirect and mediated, with computing tools, including software processes or other users, who—in turn—initiate other processes and/or use other tools.

The chain of mediation becomes longer and more complex as we move from the period of the mainframe, to the client-server world, to the internet era. In this last context, all actions are mediated actions, actions executed by processes or tools, which we can properly call “agents.” Another reality based on this transformation is that agents and persons, or users and processes are in many points undistinguishable from one another, meaning the same as a person accesses a process and a process accesses data, a process can also “access” a user in a reversed chain of events.

Given this, both processes and individuals appear in the system as agents, and both have some form of identification data attached to them. At least they have a name (a process name!). It is in the nature of things though, that names are not intrinsically attached to processes, nor users, as well as users are not attached to processes or vice-versa. In simpler terms, we can say the information technology world is essentially discontinuous, as the connections between the parts are instrumental, temporary, and external.

In our life, as consumers, citizens, or workers, we see this in action when we have different names in different contexts and use different tools to read or write similar sets of information. Therefore, user access evolves in this way, becoming more and more complex, given there is no unambiguous attachment of the user to his or her tools or to the processes and names under which these tools and processes execute.

Immediately we see the whole notion of Access Management has to evolve to consider not only the immediate act of “seeing” some data in a folder or a folder in a cabinet, but also the relationships between the agents, the names of the agents (i.e. how the agents are known in a system) and the tools or processes initiated by the agents.

We also need to consider delayed actions, meaning by that those processes that are long-running or—being mediated—execute over time and indirectly access data. Multiple users will also launch the same tool, but read or write different data sets, thereby underlining the growing complexity of access controls. Similarly, it is normal in all types of organisations that users have different authorisation levels for the same tool and the same data set, which is an added level of control that we term in the trade “fine-grained access controls,” an extra layer of access management which is itself mediated by the first layer of user authentication (i.e. name validation).

This picture can be completed by saying that for each of the transitions depicted above, moving from the individual user to stored data, passing from process to process, there will be one or more instances of “user authentication.” People and processes are authenticated by some attributes they present or have. This will become relevant in a later discussion around user authentication (name validation) and authorisation.

What needs to be highlighted here, in our analysis of Access Management, is that all user or process actions are ultimately “reading” or “writing” operations. Strictly speaking, there are only two types of security technical, material contexts: read and write. These two possible actions lie at the bottom of the two primary Security principles of “confidentiality” (associated with reading) and “integrity” (associated with writing). Out of these two, we can develop the entire logic of Access Management, and each of the Security models pointed out earlier in this chapter.

- Granting
- Limiting
- Preventing
- Terminating

Now—in light of the idea of indirection and agent action—we can say that each of those modalities will have a number of instances, for example, direct and indirect granting of access rights, as well as direct or indirect prevention of access. It is often the case that we grant access to an individual, but not to a process or tool, in which case the mediating tool also needs a mechanism for authentication and

authorisation. It is a common experience too that users lose access rights (for example their user names are invalid), but their tools continue to have permissions to read and write data.

Therefore, security becomes a far more nuanced and complex task than that of protecting a specific object. In fact, even if we retain the abstraction of “protection” and information secrecy, we clearly see that Security needs to be applied not only to the “final” object or “target,” perhaps a data store, but also to each of the agents in the chain of access.

If action becomes indirect, a chain of action along a series of agents and objects, Security also becomes indirect and “distributed” along that chain. This put the goal of Security in a different light, showing that access controls are not set on the object or target (the usual “pot of gold at the end of the rainbow”) but instead on the entire chain that leads to the object. I prefer to think that Security does not protect information itself, but the actions that either write or read data. Alternatively, we could use a much better concept of information, by understanding it not as an object or thing, but as a relationship between the user and data, or between the agent and the object.

Security in these expanded terms is Security (not only protection!) of the “act of information,” which can be reading or writing data, as well as transmitting data (we see the action from the side of the object or the origin of the data).

The four modalities of access (granting, limiting, preventing, and terminating) are moments of the information chain, parallel to other correlated conditions which have to exist in all information acts: for example, granting access corresponds to an act of trusting the user, while limiting access corresponds to an act of selectively allocating trust. This is another level of expansion, if we think of it as another step away from the idea of Security as a discipline of secrecy and protection. So there are three moments of this analysis: first we see how secrecy and integrity correspond to elementary reading and writing operations. Then we reveal how Security becomes indirect and mediated as the access chain expands. Then we understand that we are not practicing Security around some material object called “information” but effectively working on the act of information itself (which implies a relational concept of information), and finally we return to Access Management modalities, where we note that it is simultaneously a profession of trust and risk management. John Arnold has developed similar ideas in his Collaboration-Oriented Architecture papers.¹⁵

Modalities of Risk and Trust

To go beyond the risk-based, protection-centric Security stance we need to adopt a worldview that naturally combines multiple perspectives. This is similar to the change proposed by Magoroh Maruyama in his theory of transcultural epistemological types.¹⁶ The same as a unilateral, techno-centric perspective produces a Security practice focused on protection technologies, a balanced, multi-ocular worldview leads to better and more complete Security strategies and programmes. In the model I propose, there are four aspects, which are integral to Security as a whole: Direction, Selection, Protection, and Verification. These in turn can be linked to the four Access areas of “granting, limiting, preventing, and terminating” which we considered.

The dominant trend in the Security disciplines and the market is the perspective of Protection. The Verification view comes second. Distant third and fourth places are occupied by the disciplines of Direction and Selection. This sequence reflects largely the historical evolution of Security models and technologies. It is clear, for example, how protection disciplines correspond to the initial periods of IT implementation in the military, industry, and academia, while the verification disciplines prospered with the increase of legal and regulatory compliance in the decade of the 20th century. The disciplines around trust definition and allocation (Direction and Selection) are less developed and often are confused with the others.¹⁷

- Trust Definition, in this new Security Management approach, is seen as a question of Direction (Trust Definition). In this context, user identity is a matter of “Distinction” of the user among other users.
- Trust Establishment, is a question of Selection (Trust Allocation), and user identity is a matter of “Membership” of the user in some group or category.
- Trust Enforcement, becomes a question of Protection (Trust Enforcement), and identity is then seen as an “Object,” i.e. as the data objects that stand in for the user (user name, credentials, attributes).
- Trust Validation is understood as question of Verification (Trust Validation) and Identity is a matter of “Context” (meaning that an identity is valid within a context and invalid outside of it).

Trust Definition and Trust Establishment are reflected in a view of Security “in” the organisation, and they answer questions around the benefit of utilising IT technologies, trust management and user enablement. Complementarily, Trust Enforcement and Trust Validation materialise in a view of Security “for” the organisation, aiming at assurances and actions in terms of Data Control, Compliance, Protection, and Privacy.

In other words, Security “in” the organisation is the “subjective” position, the position of the business leader, the owner, the strategist, but also that of the group, the organisation, Society in general. Security “for” the organisation is the “objective” position, the position of the implementer, the controller, the auditor, but also that of the engineer, the technologist. That is the position of IT organisations in general.

It is clear the subjective and the objective positions have to arrive at different ideas of Access Management, but it is also clear these two positions are interdependent and cannot exist separately.

Security “for” the organisation revolves around processes of Trust Enforcement and Trust Validation. Overall, it can be described as Security centred on risk management. At this level, Identity Management deals with individual identity as an object and as a context. More precisely, it works on a complex combination of objects (user data) and contexts (for example infrastructures and services).

Security “in” the Organisation, in turn, moves around processes for Trust Definition and Trust Establishment, and it can be described as Security centred on trust management. This aspect of Security Management deals with individual identity as distinction and membership. This effectively means that Security here defines and allocates trust levels, depending on the identity of the individual and his or her membership into groups or roles.

Therefore, we have here four modalities of risk and trust and two major groupings. The modalities are Trust Definition, Allocation, Enforcement and Verification, and the groupings are Trust-focused and Risk-focused Security. These modalities and groupings are conceptual, but condense the basic principles of our profession. In fact, we have arrived at this model through a process that can be called “unfolding” or opening up of ideas that are present in embryonic form in reality. The complete picture of these concepts can be seen in my previous work, for example in my article “What Security Shall Be.”¹⁸

Information Theories

When opening the concept of Information Security, as we have done in the previous sections, we arrived at four perspectives of identity, as distinction, as membership, as object and as context. This is our starting point to address now - the present and the future of information theory.

Information theory needs by itself a detailed analysis that is beyond the remit of this book, so here I will point to information as it appears in the Security discipline. We have progressed towards a more correct idea of information when noting that IT Management and Security disciplines are not about an information object, but an information chain. The four Security perspectives operate on this chain from different angles and covering different but complementary concerns.

What is the origin of the “object” and “flow” theory of information that Security disciplines have taken up uncritically? I believe the objective or material concept of information is a construct that moves across many disciplines, beyond and around Information Technologies and Security. It is perhaps rooted in the physical sciences, but we need to note these, as well as mathematics and other sciences, do not have a single concept of information, and the debate is still open about the nature, the measure, and the implications of it.

I believe the current, dominant idea of information as an object is both inherited from some natural science branches, and from some particular interpretations, but it is not a general scientific concept. As it was accepted uncritically, it appeared as a “fundamental idea,” supported by science, when in fact scientific literature has not produced a definitive, universal theory about this.

An all-encompassing definition of information as an object and material flow was given by Harold Borko: “Information science is that discipline that investigates the properties and behaviour of information, the forces governing the flow of information, and the means of processing information for optimum accessibility and usability. It is concerned with that body of knowledge relating to the origination, collection, organisation, storage, retrieval, interpretation, transmission, transformation, and utilisation of information.”¹⁹ I quote this here because it reflects very closely what the technocentric Security practitioners have in mind when they speak about information.

Perhaps the most extended and used theory of information is that of Claude Shannon,²⁰ even if the author himself agreed that his definition of information covers only a minor aspect of it, the transmission of signals in noisy channels (or media). Shannon explicitly excluded any meaning or content of information. Several authors have pointed out this limitation.

For example, Ernst von Weizsäcker writes: “The reason for the ‘uselessness’ of Shannon’s theory in the different sciences is frankly that no science can limit itself to its syntactic level.”²¹

Similarly, J. Peil writes: “Information is neither a physical nor a chemical principle like energy and matter, even though the latter are required as carriers.”²²

More significant, for our purposes—in the realm of Information Security—is the opinion of the “father” of cybernetics, Norbert Wiener (1894–1964), who asserted: “Information is information, neither matter nor energy. Any materialism which disregards this, will not survive one day.”²³

Wiener’s suggestion especially should call the attention of the IT professional and lead him or her to study in more depth what the nature of information is. On the one hand, as I pointed out above, there is no established or definitive theory of information; on the other hand, major contributors to this domain agree that information is not a material object. I would also add that if it is not a material object, it does not flow.

To consolidate this idea we need to look briefly into the work by Jon Barwise and Jerry Seligman with the confusing title of “Information Flow.”²⁴ The authors present a theory based on the notion of “information flow” but simultaneously suggest that information is not an object and not a material flow: “Our primary interest is not so much in the ways information is processed but in the very possibility of one thing carrying information about another. The metaphor of information flow is a slippery one, suggesting the movement of a substance when what occurs does not necessarily involve either motion or a substance. The value of the metaphor lies largely in the question it raises. How do remote objects, situations and events carry information about one another without any substance moving between them?”

Therefore, the authors deny a material or flowing nature of information, and even posit some forms of “remote,” indirect or mediated, action, but dedicate the entire book to a “metaphor” of flow. It would have been clearer to explain that information does not flow and the inadequacy of the metaphor. I think that at least in the Security domain, this “metaphor” reveals a fundamental problem and leads to other mistaken ideas and ineffective practices.

It is not hard to follow from the need to abandon the notion that information is composed either of “bits” or “data” or “information stores,” in one way or another a set of objects in need of protection by the Security professionals.

If information is not an object and it does not flow, what is it? How did it become what it is in the current world and why has it become a matter of confusion?

Definitions of Information

Once we leave the one-sided, techno-centric approach, information ceases to be seen only as a thing or an object, and we can conceive it as something that causes a change in our conscious perceptions. In this sense, information is a perceived difference, or, as Bateson said, “A difference which makes a

difference,” i.e. a difference in the world which causes a mental difference.²⁵ This moves the emphasis from the object to the subject, from information as a thing to information because of interaction.

On the other hand, information may also be defined by change in the “mental system itself” only triggered but not caused by the external world. This leads to definitions of information that are focused on mental qualities and the ability of the mind to form ideas and images. Finally, information can be also conceived as something independent of the external world, more or less in an idealistic fashion, something living in the mind.

Humberto Maturana and Francisco Varela also deny that information is a substance: “Notions such as coding and transmission of information do not enter in the realisation of a concrete autopoietic²⁶ system because they do not refer to actual processes in it. [...] The notion of coding is a cognitive notion which represents the interactions of the observer, not a phenomenon operative in the observed domain.”²⁷

In this sense, it is possible to speak about information and assume at the same time the systems involved are autopoietic, “closed” systems that do not exchange information with the environment.

Maturana and Varela write: “Organism A does not and cannot determine the conduct of organism B, due to the nature of the autopoietic organisation itself, every change that an organisation undergoes is necessarily and unavoidably determined by its own organisation.”²⁸

According to this theory, interaction and communication are possible but not via “information flows,” as autopoietic entities do not have “inputs” or “outputs.” This line of thought is taken further by the German sociologist Niklas Luhmann in his theory of organisation: “In the context of the autopoietical reproduction the environment exists as irritation, disturbance, noise, and it only becomes meaningful when it can be related to the system’s decision-making connections. This is only the case when the system can understand which difference it makes for its decision-activity when the environment changes or does not change in one or the other respect.”²⁹

These thoughts are not isolated, and come from a philosophical tradition that does not reduce information to statistical or syntactic elements. Some philosophers go so far as to emphasise the “mental” pole of information, making it independent of the world, while others take the middle path and, like Luhmann, maintain that while there is no information flow, there is systemic coupling, i.e. interaction. Looking at all these interpretations alongside the traditional thing-like nature of information, we can begin to reshape our idea of Security and expand our understanding.

While for Shannon information is inversely proportional to probability, for Wiener it is directly proportional to probability. For Shannon, information and order are opposite concepts, while for Wiener information and order are co-dependent. In fact, for Wiener, the entropy of a system (i.e. its randomness), is a measure of disorganisation, whereas for Shannon, entropy is a measure of information (positive entropy or the number of potential choices of the sender).

These differences reveal Shannon approached the theory of information as an electric engineer, while Wiener was a proponent of cybernetics, or the theory of control, which asserts the principles of feedback and systems coupling. For Shannon the flow of information is unidirectional, for Wiener it forms a circle between the participating systems.

In the Security domains, when we speak of “risk” we usually mean information risk. For historical and cultural reasons we assume as self-evident that information is an object (a “resource”) but also that it has an intrinsic value—like a piece of gold has value--that it can be stored, that it moves between information sources and consumers, and that it needs to be protected. As I said before, these assumptions are rarely questioned and Security professionals are averse to such a discussion. In light of the critical remarks that I have documented in previous sections, I hope that this resistance or lack of interest may decrease.

The importance of this arises from all the problems around the idea of risk and Security investment decisions are linking to the underlying conceptions of information. In this chapter I summarily showed where those differences point, and in following sections I will explore how these perspectives of Security and information are aligned with four stable “world hypotheses,” using the terminology of Stephen C. Pepper.³⁰

We will see that beyond the idea of information as an object, a substance that flows and can be stored, Security architectures and programmes can be designed around other paradigms that do not take information as a substance. Speaking about the four world hypotheses he observed in philosophical thinking, Pepper used the term “mechanism”³¹ to refer to those tendencies that relied on mechanical metaphors around simple or complex machines. The mechanistic metaphor is indeed in the foundations of computer sciences and we in Security only inherited that position.

Different approaches to Information Security will arise if we change our notion of information, from the mechanistic hypothesis to a different one. For example, the sub-disciplines of compliance are based on metaphors of context and history--Pepper called these “contextualism”--but moving from one metaphor to another is not what I am proposing here. Equally, we could adopt other metaphors but still have unilateral views of our work and our goals.

Real change will come when we aim for what could be called a “fifth hypothesis”³² which would articulate the other four in a non-eclectic manner. Starting from there, we should analyse and disentangle the “established truths” of our profession, as we have done with the idea of information. When doing that we immediately notice that our philosophical approach is also valid for other accepted ideas, for example that of the “value of information.”

Many assumptions and ideas hinge on this notion. After all, everything that we predicate for the disciplines of Access Management depends on the idea of “value” - more precisely, on the idea that we are protecting or managing access to valuable resources. Without the associated idea of value, there would be no reason for the Security practices and for the methods of “risk assessment.” As it happens with the theory of information, Security professionals do not talk about the value of information. The

“value” of information is an absolute given—another presupposition—that remains hidden from critical thought.

Sometimes we refuse analysis and questions because even the thought of these leaves an uncomfortable vacuum and threatens to undermine our professional identity and our work environment. I have seen talented professionals, highly educated and articulate, leave this kind of debate abjectly declaring they would not discuss anything that put their jobs into question. I am sorry to report that this does not sound like a good basis for professional ethics.

As we have seen, risk analysis is part of a line of thinking that depends of the notion of value of information, and information itself is articulated around a mechanistic ideology. From this, we may infer the concept of value is also a mechanistic and techno-centric idea far from the economic and sociological guidelines that should illuminate our work.

In a different chapter, I will address how the four perspectives interpret value, and where we can surpass the techno-centric stance, but now let us look into the effects the new approach will have on the Access Management disciplines.

Here I want to introduce the concept of assurance, which is relevant to complete our analysis of Access Management. In this, I follow the Arca Systems approach distinguishing Security Assurance from risk-based concepts.³³

Now let us consider as a tool Kan Zhang’s “secure system” model, where a completely secure machine or system is described as one that allows no information exchanges (this still within the mechanistic metaphor of flows of information).³⁴ This imaginary system was proposed to explain how a Security policy effectively **reduces** the “security” of a system by granting access to it. Granting access, in this model, increases the Security risk. This thought experiment shows the entire conceptual framework of traditional Security at play: Security expressed in terms of object and flow, Access Management formulated as null access, i.e. as absolute “protection” of the object, and risk expressed in terms of increased access and reduced protection.

If we now return to the suggested definition of assurance, we can immediately see such a scenario is not compatible: a high assurance rating is not compatible with a high Security rating.³⁵ Indeed, without any information flow (i.e. “highest” protection), there is no way of measuring assurance, because it depends on user needs and actual use of the machines or networks of the IT system. This means that Security defined in terms of the object may not express and manage all the possible instances of Access Management, leading to contradictory and paradoxical results. Assurance can be defined as confidence in the controls, for example in the fact these are granting, limiting, preventing, and terminating access at a suitable level and to accepted individuals or groups; but it is more useful to define assurance as confidence in the result of applying the controls, i.e. in the information they generate over the system under observation.

If the system is isolated, then all controls, from any definitions and scopes, will not produce useful information about the system or its isolated users, and therefore there cannot be any assurance. Paradoxically we would still be able to say the system is "secure" in the sense of being encased, protected and beyond most conceivable threats.

Reducing uncertainty and increasing assurance in a system under Access Management requires setting up known policies for granting, limiting, preventing, and terminating access, as well as fool-proof methods of access data aggregation, including data on the security components themselves. This is a conception of Access Management, one that is not focused on "protection" in itself.

This is the most important conclusion up to now: Information Security shall not hinge on "protecting information," but on generating high assurance levels, which in turn demand good quality information about the organisation or system under consideration. The system—from this point of view—is a chain of actors and objects linked in interaction and the task of security is to direct, select, protect, and verify those interactions. Only at this level can we speak of having "control" over the secured system as a whole!

I think the debate would deepen and change if we adopted a multipolar philosophy, on the lines of Pepper's four World Hypotheses. Individually, we may or may not change our root metaphors, our essential hypotheses or views, but we might start considering there are other concepts of Information, other ideas of Security, and therefore other ways to approach our professional tasks in general, and Identity and Access Management in particular.

While in the past security was mostly associated and even attached to the "protection" ethos, a complete and a more business-centred vision allows us to develop other complementary strategies. It is essential to understand there is no Security without business direction, especially without the definition of what the business model calls for as a circle of trust. The business policies come first, and the definition of what we want to have as a trusted environment is a precondition to all the rest.

Overall, then, the need for Identity and Access Management processes is part of the growth of the security disciplines, and their increased linkage with business concerns. While the first thrust of Security solutions was mostly technical, recently there is increasing emphasis on performance and economic considerations, and these depend on business process transformation.

¹ A definition of security: "...protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction," according to the U.S. Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542.

² Official (ISC)2 Guide to the CISSP CBK, "Information Security and Risk Management," 2006

³ The standard approach to informational assets: "The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets." – NIST "An Introduction to Computer Security," 1995

⁴ "Controlling access to systems, services, resources, and data is critical to any security program. Without a comprehensive approach to control access, there are few options to managing the security posture of an organization. The ability to clearly identify, authenticate, authorize, and monitor who or what is accessing the assets of an organization is essential to protecting the environment from threats and vulnerabilities." -- Official (ISC)2 Guide to the CISSP CBK, "Access Control," 2006

⁵ A security model is a formal description of a security policy.

⁶ D.E. Bell, L. LaPadula, Leonard J. "Secure Computer Systems: Mathematical Foundations" , 1973

⁷ K.J. Biba, "Integrity Considerations for Secure Computer Systems," 1977.

⁸ Defined by the "Trusted Computer System Evaluation Criteria" (TCSEC), 1983

⁹ D. Clark, D. Wilson, "A Comparison of Commercial and Military Computer Security Policies," 1987

¹⁰ J.A.Goguen and J.Meseguer, "Security Policies and Security Models," 1982

¹¹ For example "reading up" or "writing down" actions.

¹² D. Sutherland, "A Model of Information," 1986

¹³ Meaning objects with higher or lower levels of protection.

¹⁴ J. McLean, "Security Models and Information Flow," 2003

¹⁵ J. Arnold, Collaboration Oriented Architecture – Securing a De-perimeterised Enterprise

https://docs.google.com/document/edit?id=1IEVxlJesGn7h_vK1pa4yvYjXY59ERtVqzn6yVvX6mAlaM

¹⁶ Page dedicated to M. Maruyama's work: <http://www.heterogenistics.org/maruyama/personal/biography.html>

¹⁷ See C. Trigos, "Four Perspectives of Risk and Trust in Cloud Computing," 2011 <http://carlos-trigos.com/public/four-perspectives-on-risk-and-trust/>

¹⁸ C. Trigos, "What Security Shall Be," 2011 <http://carlos-trigos.com/2011/04/04/what-security-shall-be/>

¹⁹ H. Borko, "Information science: What is it?," 1968

²⁰ C. Shannon, "The Mathematical Theory of Communication," 1964

²¹ E. v. Weizsäcker, "Offene Systeme I – Beiträge zur Zeitstruktur von Information, Entropie und Evolution," 1974

²² J.Peil, "Einige Bemerkungen zu Problemen der Anwendung des Informationsbegriffs in der Biologie," 1971, 2007

²³ N. Wiener, "Cybernetics," 1968

²⁴ J. Barwise, J. Seligman, "Information Flow – The Logic of Distributed Systems," 1997

²⁵ Gregory Bateson, "Steps to an Ecology of Mind," 1972

²⁶ An autopoietic system is defined as a system constituted by processes interlaced in the form of a network of productions of components, which realise the network that produce them and constitute it as a unity. An autopoietic system is a closes system, and it exhibits the property of "self-reference" according to Maturana and Varela, i.e. the ability to operate as a self-organising system.

²⁷ H. Maturana, F. Varela, "Autopoiesis and Cognition: the Realization of the Living," 1973

²⁸ H. Maturana, F. Varela, "Autopoiesis and Cognition: the Realization of the Living," 1973

²⁹ N. Luhmann, "Organization," In Kupper and Ortmann (Ed), Mikropolitik, 1988

³⁰ Stephen C. Pepper, American philosopher, 1891-1972

³¹ S. Pepper, "World Hypotheses – A Study in Evidence," 1942

³² Bill J. Harrell, "Five World Hypotheses," http://people.sunyit.edu/~harrell/Pepper/pep_wh-select01.htm

³³ See: D.J. Landoll, R. J. Williams, "An Enterprise Assurance Framework" - Arca Systems, Inc.

³⁴ K. Zhang, "A Theory For System Security," Cambridge University, 1997

³⁵ J.R. Williams, G. F. Jelen, "A Framework For Reasoning About Assurance" - Arca Systems, Inc., 1998. See also: J.R. Williams, G. F. Jelen, "A Practical Approach To Improving And Communicating Assurance" Arca Systems, Inc. - <http://www.aspectsecurity.com/documents/Arguing.pdf>

4. The Context: Identity becomes Data

Data-Centric Security

Security architects and practitioners need to develop an integrated data model that will enable end-to-end user management and access control. I proposed this approach in 2006 and advocated a data model that could become the basis for the next period in Security and Identity management.¹

There have been important changes in the Security disciplines in the last decades; we have seen important transformations from the origin of these disciplines in Government and military sectors. For example, now we have an image of IT and Security as a complex of “processes,” similar to other business areas.² Security definitions have moved through several stages, passing from the early association with perimeter protection, to security education and risk management, and moving now to an emphasis on compliance and auditability.

On the negative side, these steps have not been reflected in all domains of our professions. The more recent business “alignment” ideas are still restricted to the management consulting branches, while the majority of the Security specialists still move within the “perimeter protection” ethos. While we know where to position Security in the general picture of enterprise and public organisations, it is not clear what to do in specific areas. The newer sub-disciplines like Identity Management suffer much under obscure definitions and stale ideas. From the “outside” of the Security disciplines, for example from the ITIL and COBIT practitioner domains, some help has come by linking security into the wider concerns of business and technology management.³ These valuable contributions, nevertheless, while collating all the aspects and key indicators of Security, are nevertheless insufficient to solve other problems of principle and practice. These we need to address and solve by ourselves.

As a result, many business leaders are aware of the relevance of a security process, but mid-level management and technical personnel are in the dark about how to connect business models and objectives with their own practice.

Enterprise and organisational security is not only about “information security” as we learned in our training and our schools. The time where information was “discovered” and hyped as a “business resource” is over, and Security and Identity management are not restricted to “confidentiality, integrity and availability” anymore. As I have suggested in previous sections, it is now essential to blend Security principles and actions to a systemic view of the organisation. A key step in that direction is to link Security and Systems Management disciplines to achieve common economic goals of performance and efficiency.

That association is already reflected in much of the thinking around “Security as a service” and “Security in the Cloud,” both of which need a deeper integration of Security and Information Systems. To progress from there, we need to look now at the sub-domains within Security

management, following the example of the ITIL disciplines, articulated around Service Support and Service Delivery and their respective areas. In the previous section I suggested that a good subdivision of Security would be that between Risk Management and Trust Management. This will also help bridge the gap between the business models and Security practices.

Here is how I think we should proceed. The root of Security Management is a data structure. Although simple at the core, its ramifications are complex. Security Management (Risk and Trust Management as a whole) relies on a series of data associations or “mappings” as we would say in software development terms. A non-exhaustive list would be as follows:

- Users to user names
- Users to passwords
- Users to tokens
- Users to certificates
- Users to accounts
- Users to groups
- Users to roles
- Users to services
- Users to processes (or agents)
- Users to operating systems
- Users to devices
- Users to locations
- Users to objects
- Users to permissions
- Users to audit events

Together, these mappings form a single data type at the core of all security technologies. This is not exactly what technology vendors tend to call “data-centric security”—another trendy name for “data protection”—but a cross-domain approach to all Security domains: Application, Identity, Infrastructure, Networks, Compliance, and others. This fundamental step will allow us to see enterprise and organisational solutions beyond the traditional “point solutions.” My thesis is that only this approach answers the need for efficient and secure data management across technological and platform boundaries.

This is a first insight for the Security practitioner and the expert technologist: Security needs information integration. Without this, what we have is a collection of trendy but disparate products and “solutions” that need a few years if not months to become obsolete. These isolated solutions may be more or less effective, but on the whole do not increase trustworthiness of the IT services, and instead multiply risks and uncertainties at great cost for the organisation.

A data-centric approach would learn a lot for the standard disciplines of Information Architecture. Instead of the path followed by the various versions of Security Information Event Management

(SIEM), still focused on the attack-defence paradigm, a proper data-centric Security would focus symmetrically on trust enablement and risk reduction. This means that it would collect, aggregate, analyse and communicate events related to performance as well as detected Security violations. There are aspects of this approach in various technologies in the market (some even in the Identity and Access Governance branch or IAG based around role-based access controls), but a complete data model is still unavailable.

What is a Security Policy?

Let's look at the theoretical underpinnings of the proposed approach by using some academic results summarised by Kan Zhang at Cambridge University.⁴ Zhang adopts as a starting point the notion that a "completely" secure system is one that does not allow the flow of information. Note that this model is strictly within the idea of Security as "protection" and "prohibition," and also adopts the notion of information as "flow." The important aspect, though, is that this starting point allows us to see how even in the standard theory (well represented by Zhang), a secure system is not one that has a well-defined and controlled Security policy, but one that does not have a security policy at all.

To understand this, we need to analyse the standard reasoning closely. If a completely secure system is one for which no "information flow" is allowed, then it follows that any "Security policy," by opening up certain levels of access, will necessarily detract from the original completeness of protection. This is so because a Security policy can only specify which information exchanges are valid. A security policy (an access control matrix, for example), does not transform "insecurity" into "security," but instead brings the Security level to a defined and/or accepted level. If the Security policy is well defined, then the factor of decrease will be a "known quantity," or so the standard theory goes.

I believe that an acceptable, consensual definition of Security policy is that it represents an instrument (a formal, approved document) which maps users or processes to other individuals or processes. I rely on the reader having seen my definition of Access Management in the previous chapter, and how all access is mediated access for reading and writing operations. Mapping users and entities in the system sets up its "security policy." By this mapping, users are able to interact with information sources, and information sources are able to reach users (or their agents). These relations can be seen as exchanges of information inside and outside of the system.

Normally even small organisations have multiple user registries, and various classes of users. This is part of organisational life and cannot therefore be classified as a problem. The problem arises not from the variety of users or the data they consume and generate, but from the diversity and combination of mappings between users and their resources (for example applications, web services, e-mail servers, files, networks, and so on). Again, by a systemic understanding of Access Management, we should see that a Security policy does not implement only "protection" measures, but actually channels that assign levels of trusted access to specific users and groups.

A good Security policy then, even starting from the standard theory, is one that reduces "protection" levels selectively according to the business model, i.e. the trust boundary of the organisation. We

certainly need solutions that are able to tell us (and the enterprise and organisational leaders) when a user is accessing a specific resource for what purpose, but the same emphasis should be put on knowing if the trusted users are using the information channels that are intended for them. In other words, we are back to the symmetrical model of Risk and Trust management.

The standard Security technologies, still focused on protection, put us in a position where--by collecting and analysing all user access information--we can disallow invalid changes, and to roll back these changes after a security breach. Data-centric Security though should go further and promote, speed up, simplify and perform information exchanges that are predicated by the organisational and business model. To understand this transformation it is essential to mark a distinction between the ideas of "information assurance" and "information risk."

The Security practitioner and the technology expert rarely consider these terms philosophically. We have already analysed in previous chapters how weak our definitions of "risk" are. It is also clear that we do not have balanced definitions of "trust" and "risk" but have seriously confused semantics around these concepts. A good test of the lack of clarity of our conceptions is that we rarely find an expert or a Security practitioner that will vouch for his or her own solution, always expressing these in cautious and hedging terminology. In other words, we as a profession are reluctant to speak about "assurance" in our metier.

Security experts like to speak about "secure" and "insecure time."⁵ Insecure time is the period where the Security policy has failed to stop intrusions or malicious use of "information." This corresponds to a realistic school of thought, erroneously called "pragmatic" school, which believes that a system is secure if its "secure time" is greater than its "insecure time."⁶ I cannot deny there is very sensible advice in this position, as it helps to move the specific technologies into the background and focus on a more holistic view of the organisation. From the point of view of the business leader, it does not matter how you increase secure time versus insecure time. What matters is that you achieve good results. On the other hand, this definition lends itself to serious managerial misunderstanding, because there is no transparent way to determine when there is "too much" insecure time in a system or organisation. Let's remember our previous result by which a Security policy effectively increases "insecurity" by enabling access channels and this will allow us to understand the comparison between secure and insecure time cannot be quantitative. In other words, the proportion of access and trust allocation and prohibition and risk avoidance is not a matter of rough numeric balance, but only the product of a conscious, deliberate, planned, determined decision rooted on the business model.

To achieve assurance, then, means to assure business objectives and not Security objectives, specifically Security assurance does not imply a maximum of "secure time" but certainty that we are achieving the level of access we have adopted as part of the business model. Transitioning to this stance requires addressing the entire life cycle of the organisation's information systems, covering all its internal and external channels of interaction. For this, the best designs will be those that encompass all user mappings as mentioned before. This requires a switch from "feature implementation" (the techno-centric view) to "integration" work (the

service-oriented architecture view), seeing each Security initiative as a data-centric project, as a data integration task.

Security Assurance

For too long of a time, it has been trendy to speak about information as being the “lifeblood” of the enterprise.⁷ Equally easy has been the position of Security management as a special, even separated speciality in the context of Information Technology. However, historical transformations are making Security very similar to Systems Design and Management. For example, in the same way as the systems management database (also known as CMDB or Configuration Management Data Base) contains item dependency and inclusion mappings of the ICT systems, there is a nascent concept of a Security Management Database implicit in the disciplines of Security Event Information Management and Security Analytics.

Information interaction, bi-directional and multi-directional exchanges are part of the economic process, and information systems are part of the business infrastructure. While this is evident, an atmosphere of mystery and strangeness persists around Security, as we do not understand the fact discussed above: the most secure system is one that does not exchange information with the environment, while a system with a security policy is relatively more insecure. This paradox has driven many professionals to try to cancel the “problem” by proposing more security technologies, additional standards and processes, without caring for the overall meaning of Security in the organisation. With this rush towards supposedly new solutions (while we all know that nothing new has appeared in the security technologies in the past 20 years or so), we have just increased the fragmentation of the IT environments and have also introduced more complexity and dangers for the organisation. With this attitude we, the Security practitioners and experts, have effectively created our own problems.⁸

If instead we position Security Management at the same level as Services Management, following the example of the ITIL, we will be able to define the Security sub-areas in a very clear fashion. This in turn will clarify the skills and activities of the various Security practices.

In a recent article, I proposed a four-layered model to reorganise the Identity and Access Management domain according to this philosophy.⁹ Other experts classify the Security and Identity disciplines in various manners, but with a common method consisting in listings of activities that can be easily seen in our practice. For example, a group of professionals based in the South of England recently published an approach to security process maturity defining five key areas¹⁰:

- Protection: Perimeter security, intrusion detection
- Validation and Provisioning: User to username and password mapping, user to accounts and services mapping
- Access and Integration: User to groups, roles and objects mapping
- Compliance: Compliance with the law, individual rights and policies
- Total Security Confidence: A continuing process of measurement security improvement

These sub-processes are seen simultaneously as phases in time, layers in organisational security, and parts of the total picture. They form an integrated Security Management process. The problem with this approach is that further classifications and refinements are always possible; for example here is a more detailed breakdown (which is one I adopted up to 2006)¹¹:

- Protect: User platform to network mapping
- Detect: User to protocol and network layer mapping
- Validate: User to user name and password mapping
- Provision: User to services and accounts mapping
- Authorise: User to groups and objects mapping
- Integrate: User to roles mapping
- Verify: User to security policies mapping
- Audit: User to logged event mapping
- Manage: User identity and access management policies and risk management
- Improve: User identity and access management continuous improvement

The advantage of the second listing is the guiding principle, associating data mappings with each of the sub-disciplines. For example, the first process (Protection) maps the user platform to the network, because security practices at that level focus on hardware and infrastructural measures. Further analysis would give even more detailed pictures of the Security sphere, but this does not solve the problem. In my opinion, we need more than analytical approaches, i.e. more than classifications. A dual approach is necessary, both synthetic and analytical, to first determine the most meaningful “parts” of the Security practice, but also to organise these into a logical, coherent structure. The solution that I propose is to align the security disciplines with the Fundamental Conceptions of Information that are at the core of this book. My work on this matter leads for example to the concept of “eclosion” in Identity Management, by which I mean an “opening” or “unfolding” of the Security concepts around the four basic perspectives of Direction, Selection, Protection and Verification.¹²

Following this path, we arrive at an idea of Security assurance that is far from hype and trends. This idea of Assurance is not new though, and actually arose in earlier periods of IT academic work. The best exponent of it was Jeffrey Williams,¹³ of the Canadian company Arca Systems. I have adopted his notion of assurance as a measure of confidence in the accuracy of a Security measurement and not a measure of the degree of “satisfaction.” As Williams explains,¹⁴ a measure of satisfaction would depend on measurement of the security needs, but how do you measure what you need so you can measure what you do to satisfy it? As I indicated in a previous chapter, the most disturbing problem in standard risk analysis is that it does not consider how risk assessment itself changes the security needs and profile of an organisation. While there are many ways to express risk quantitatively, objectively or subjectively, there is none to express “security needs.” So, by assuming a theory of assurance as “satisfaction,” we originate incomplete, obsolete, costly and problematic solutions.

Assurance is orthogonal to risk. They are different dimensions and should not be confused, because a high assurance rating is not equal to a high security and low risk rating. In the “secure system” model, let us remember, there is no information exchange. No information “goes in” and no information “goes out” as the standard model would admit. Is that scenario compatible with a high assurance rating? It is not, because if no users have access to the assets, this cannot represent any “security needs.”

Equally concerning is that, if a system has strong access controls but lacks auditing functions, how can we tell whether the installed technologies are functioning properly or at all? If we confuse assurance with security, the system will appear to be safe, while in fact there is high uncertainty about its state! Assurance, instead, has to be conceived as a measure of confidence on the information about information security, meaning by that a second or higher order of information.

Separating assurance and security becomes especially interesting when we consider the needs of the decision-maker also following the work by Arca Systems. After making a risk assessment, a decision-maker may have a quantitative idea of the risk level, but what happens if the confidence in the information gathered is low? Have we not seen innumerable cases where we and the business leaders we advise are not sure whether the risks noted (within the traditional model) are acceptable or not?

If confidence in the security information is high, then it may be sensible to add new security mechanisms. If the confidence is low, adding a new tool will increase the uncertainty in the system and potentially create new Security issues. To address this it is necessary to work out the assurance level aiming at a second degree of insight and investigating how certain our perceptions of the state of the system are.

The assurance theory I am summarising here shows the trend to multiply the technologies and services employed to enforce “security,” claiming to address uncertain or imagined levels of threat are more a problem than a solution. Most security products and services converge on the protection and verification sub-disciplines, but by doing this, vendors and consultants are answering to short-term preoccupations of business managers. It seems always easier (and less expensive) to secure one perimeter after another, than to discriminate the assurance levels of a large number of applications and communication networks.

We just need to ask the Security teams in any organisation how they are collecting and analysing the information sources provided by the IT infrastructure and the Security technologies, to understand how underdeveloped these processes are. If this is the case, what is the level of assurance that we are working at? With this we have a better context to understand the reactive insistence on risk management and the prevalent refusal to abandon risk-based security. A move towards a combination of risk and assurance does not mean leaving risk concepts behind, but putting them into a business perspective: what do we really know about our security position?

Reducing uncertainty in a secured system always requires setting up known channels of information and fool-proof methods of data aggregation, including—most importantly-- data on the security components themselves. Data flowing through those channels is meta-data (or second order

information, as I said in previous sections). A single meta-data format is possible and necessary for each assurance level and information channel, building on the idea of mapping users to a variety of business objects. I understand this meta-information as the only source that can reduce uncertainty in the organisation and its security implementations. Meta-information or “second order” information can also be seen as “positive evidence,” as compared with the “negative evidence” that we can obtain from intrusion detection and security incidents or breaches. Positive evidence increases “secure time,” to use the standard language, while negative evidence increases uncertainty.

Starting from these ideas, it will be possible to design and complete Security “assured solutions,” contrasting with the lack of guarantees usually found in commercial security implementations. A similar lack of contractual assurance is usual in software offerings, as vendors are “not responsible” for the failures and limits of their products, but this is becoming less and less acceptable as the IT markets mature and adopt new business models themselves. To assure a solution in an uncertain environment, with increasing dangers and continuous economic and social change, we need to start by understanding that information security is not a technological matter, and the levels of “insecurity” in a system depend directly on the “security policies” that we apply, while Security management ultimately consists of user management processes.

Against the present dominance of point solutions and technological silos, we will finally see Security management as a cyclic change process, adjusting to the changes of the organisation, enabling and improving other business processes, and at the same time providing a decreasing unit cost and higher performance.

Internal and External Actors

In the decades since the rise of the electronic computer era, a constant factor of change has been the expansion and diversification of the categories of users. The initial use of computers was circumscribed to scientists and engineers developing the first computing engines in a handful of laboratories. In time the types of users extended, and a division of labour took hold, with different “levels” and use patterns. This change has been continuous and we are far from seeing its end. Currently the types of users accessing enterprise and organisational information sources are very diverse. Here is an incomplete list of what we see in the field:

- System owners or application owners
- Managers (line managers or department managers)
- Employees (staff, including many types of users)
- Contractors (temporary personnel)
- Consultants (temporary personnel from consulting services)
- Services (service suppliers including cloud-based and hosted services)
- Partners (including joint venture management and personnel)
- Suppliers (management and staff of the supply chain network)
- Researchers (scientists, academics, researchers of public or private entities, also individual experts)
- Officials (members of government agencies and regulators)

- Corporations (corporate customers' management and staff)
- Consumers (private customers)
- Distributors (distribution channels' management and staff)
- Third-party customers (customers from partners and other sources)
- Visitors (unidentified or unauthenticated visitors to shared resources)

Any experienced Security professional will in fact state that this list is incomplete, lacking in detail for example, as it is common for national and global level corporations to have not only a wider but an ever-widening classification of users and potential users of their informational channels. In many if not all cases, this widening range of users is a product of a deliberate business strategy to either reach out to other parts of the population, or else a result of business acquisitions, mergers, contracts and projects that are part of the growth process of the enterprise or the organisation.¹⁵

Simultaneously with this change, we see the disappearing “boundary” or the external border of the organisation. This has been widely studied by the Jericho Forum under the concept of “deperimetrisation.”¹⁶ In relation to this, it can be said that both public and private organisations do not have an “internal space” anymore, with respect to information exchanges. For example, in IT-mediated transactions, users operate as customers of organisational services, and customers appear as users. Some organisations, recognising this trend are effectively using the same infrastructure and Security solutions for “internal” and “external” users.

What is most relevant for my argument here is that this “deperimetrisation” of the organisational and enterprise space forces us to look at all types of users and all their access routes (i.e. their interaction channels) as a common ground where the differences are not in the “identity” of the users but in what the users do in the various segments of the organisational network. As the British academic David Chadwick put it: “It does not matter who you are but what you can do.”¹⁷

To complete this panorama we need to take note too of the fundamental changes in the numbers and the correlation of external versus internal users. It is normal to find now public and private organisations where the number of external users is 4 or 5 times larger than that of the internal (staff) users. Indeed, in public organisations the disparity is many times larger in some cases as the user population is spread across entire nations. Some people say that in fact public organisations never had an “external boundary” in this sense.

Certainly, as this trend progresses, there will be a complex of identity schemes inside and outside of the organisation. Some will have weak assurance levels (or “identity proofs”); some will correspond to high requirements for assurance and authentication. In the whole, these combinations will increasingly appear as a transformation of the Security and Identity landscape, where the central aim of the IT services will converge on the management not of users, but of platforms. In more formal terms, as the complexity of user types, locations, routes and credentials increases, as the proportion of external to internal users changes in favour of the external users, the entire endeavour of “securing” the organisation and its informational resources becomes one of managing information itself.

By this I mean managing information about the users of information channels and also about these channels in all their complexity. Because of economic, social and organisational transformation, we have entered a period where Identity becomes Data; to put it in striking terms, useful to understand what our new goals are. The work of the Jericho Forum around Collaboration-Oriented Architecture is also relevant.¹⁸

I have written before about expanding the concept of identity.¹⁹ On the same lines and under the trends reviewed in the previous section, the concept of identity will develop, unfolding into a variety of internal and external "identities" for all types of organisations. It is important to explain here that this conception assumes there is no single identity that can be associated to a natural person (a biological individual). In practice, both industry and government need to rely on a combination of identification instruments or credentials, including biometric data, to compose and integrate a "known identity."

Particular levels of integration or composition of these credentials are acceptable or valid for specific business or personal transactions. For example in the UK it is normal to use a utility bill and a driving licence to buy a new phone contract. In other countries, with a national identity card, sometimes various credentials are embedded in that instrument.

So when writing about a variety of identities I do not refer to biological or personal identity, but only to identification instruments or events that serve as tokens of proof in public and private exchanges. This corresponds to my view that we are moving from "identity" conceived as an object (a thing) to "identity" seen as a subject and a membership in a relationship. In this sense, each identification instrument is a symbol of a particular relationship the individual holds with different organisations, institutions, countries, partnerships, and other human associations.

Secure Identity Management is Data Management

Another shift in understanding is necessary once we perceive the complexity and the high numbers of users we are reaching in the sphere of Security and Identity management. My take on this matter is that we need to apply ideas of performance and event management to master the new tasks. As Identity management and access control extends and changes in depth and form, the traditional approach centred on single-minded and simplistic "one-size-fits-all" mechanisms will cease to exist. It will become evident these mechanisms are in reality the source of many Security disasters.

We should instead develop Security tools and processes by applying computing capacities to their full extent to data management. After all, the computer era is all about performance in data management and nothing else. I am not chiefly speaking about cost here. It is well known that event management in the support disciplines has a cost reduction driver; for example, by handling millions of events per day in automated or semi-automated ways for data collection, aggregation, escalation and reporting. At a rate of about £1 per processed event it is easy to see that event management (translated to security event management) can bring important cost reductions; but the main point is that security event management has multiple benefits beyond cost reductions. The most critical benefit is the complete

transformation of the Security emphasis, moving from passive-defensive compliance and “risk-based” measures to active, trust and risk-balanced solutions.

It is important to recognise that this area is not empty of progress, as we have seen the development of log management, event management and security analytics products. What is necessary now is to bring all these capabilities together and rearrange them under a better philosophy of identity management as intelligent data control. The new view of Security and Identity management will be focused on mastering the complexity of access routes and data movements between the sources, registries, directories, provisioning systems, access controls and applications or services. This direction will make Security operations similar to the manufacturing steps between raw materials and purchasing, production, inventory, service and packaging and conveyance to the consumers.

In the same manner, Secure Identity Data management must have the following characteristics in common with standard enterprise data management:

- Data Governance (organisational assurance and accountability)
- Data Extraction (data collection and extraction model from physical sources)
- Data Publishing (data standards and contracts for distribution)
- Initial staging (standards and locations for data storage)
- Data quality (validation criteria and processes, data cleansing, and data quality model)
- Clean staging (standards and locations for data storage of clean data)
- Transformation and Enrichment (standards and contracts for data transformation)
- Staging or Publishing or Loading (standards and locations for loading)
- Loading (loading, updating model)

When considering this fundamental shift, we need to return to early academic results which anticipated what we are seeing now²⁰ regarding organisations as “information processors.”²¹ This view, which I still follow except for the view of information as a material flow, shows the capacity of an organisation depends on its structure, its decision-making capabilities, and the ability and experience of its people. In this perspective, it will not be difficult to bring to the foreground areas which have been investigated for many years in other aspects of business and public management, for example the relatively “old” concept of Data Governance. It is not difficult to understand that identity data must have a series of functions and processes around its:

- Data sources
- Data extraction or acquisition
- Data processing
- Data presentation
- Decision making (authorisation processes)
- Data custody
- Data delivery
- Data usage

When emphasising a data-centric approach, it is vital that this change in perspective does lead to focus only on the performance-related aspects of the problem. Efficiencies in data management are definitely at the forefront of the proposed change in direction, but equally important are the qualitative aspects of Security and Identity management. I will cover the cost management aspects of these processes in a later chapter of this book, but first let's look in more detail into the data quality criteria that we should apply.

Data Quality Criteria in Security Management

Once we adopt this new thinking, it becomes clear the essential --I would say "classical"--- ideas of enterprise and "information architecture" data management are applicable to our remit. This is one more area where the "strangeness" or "uniqueness" of Security is disappearing and has to disappear to convert it into a suitable business operating partner of the organisation. The studies covering data quality and information architecture are so diverse in theme and depth that I can't summarise all their aspects here. As a more synthetic starting point I refer the reader to the work by Richard Wang and Diana Strong published by the Massachusetts Institute of Technology.²²

Wang and Strong propose a schema that aligns very well with my own approach to Security Management (i.e. the categories or perspectives of Direction, Selection, Protection and Verification). After studying many data quality dimensions they proposed four categories: Intrinsic, Contextual, Representational and Accessibility Data Quality.²³

Each of the categories summarised several dimensions as follows:

- Intrinsic Information Quality - representing Accuracy, Believability, Reputation, Objectivity, Consistency, Completeness, Precision, Reliability and Correctness
- Contextual Information Quality - representing Relevance, Timeliness, Amount, Currency, Detail, Comprehensiveness
- Representational Information Quality - representing Understandability, Interpretability, Consistency, Arrangement, Appearance, Comparability, Compatibility
- Interactional Information Quality - representing Accessibility, Security, Availability, Usability, Convenience, Locatability, Privacy, Delivery

We could draw some immediate parallels with the Security perspectives; for example observing the link between "intrinsic information quality" and the disciplines of Security Direction. Equally important is the connection between "interactional information quality" and the disciplines of Protection. While that is worth continuing, more important at this point is to highlight that information qualities are needed at two levels by the Security disciplines and by Identity management in particular. First, we need information quality measures for the information we handle extracted from managed systems

and user registries, and second, we require also information criteria for the information we produce and transmit inside and outside of the organisation.

For this reason it is not only important to see that we are managing data, as an “external observer” or entity handling “data flows” in the organisation, but we are also an observed observer, i.e. a source of information for the enterprise or organisation decision-makers. Data quality criteria are 100% applicable to Security information sources as well as to Security outputs, but this is precisely an area that needs urgent development, as few organisations have any integration between these two concerns. Looking into the collection and analysis of information sources, we see that this domain is largely elementary and driven only by yearly audit calendars. The second level, where Security systems themselves become a coherent source of information and work to reduce uncertainty in the organisation is still in the future.

This last assertion needs some qualification. It is true that –within the silo and point solutions tendency– some departments and some applications or systems do have “security information systems” in many organisations. So when I put forward a negative assessment of the current status of Security and Identity data management I am not referring to these fragmentary, technology-centred approaches. We need to set our aims well above the current patch-as-you-go paradigm and the never-ending “technology upgrades” and achieve excellence in our professional work. I think that we have been accustomed for too long to a state of mind where we manage failure instead of managing for excellence.²⁴

In the Security professions, adopting an integrated data model and information quality criteria as described in this chapter shall signal a major step in that direction.

¹ Carlos Trigos “The Path to Assured Security Solutions,” ISSA Journal, 2006

² Paul Evans, “Information Security as a Business Process” , IT Network Solutions, 2004

³ Cazemier & Overbeek, “ITIL Security Management,” Office of Government Commerce, United Kingdom, 20th April 1999

⁴ Kan Zhang, “A theory for Systems Security,” Cambridge University, 1997

⁵ Amit Singh, “A Taste of Computer Security,” <http://www.kernelthread.com/publications/security/> , 2004

⁶ More precisely, insecure time is the sum of the time it takes to detect an “incident” and the time it takes to react to the incident (over all incidents in a given interval).

⁷ See: HP Neoview Enterprise Data Warehousing platform

http://www.hp.com/hpinfo/newsroom/press_kits/2007/business technology/brochure_neoview4AA0-7932enw.pdf

⁸ See: <http://carlos-trigoso.com/2011/08/31/iamaas-is-not-saas/>

⁹ See: <http://carlos-trigoso.com/2010/09/12/iam-more-than-people-process-and-technology/>

¹⁰ Stuart Wilson, Chris Ayres “Modern Business Challenges – Compliance and Total Security Confidence,” Pirean, 2005

¹¹ Carlos Trigos, “The Path to Assured Solutions,” ISSA Journal, 2006

¹² Carlos Trigos, “Eclosion: The Future of Identity Management” <http://carlos-trigoso.com/2010/12/22/eclosion-the-future-of-identity-management/>, 2010

¹³ J. Williams, “A Framework for Reasoning about Assurance,” Arca Systems, 1995

¹⁴ J. Williams, D. Landoll, “An Enterprise Assurance Framework,” Arca Systems, 1996

¹⁵ Adrian Seccombe, “Identity the New Perimeter,” Surrey University, 2010

¹⁶ See the Jericho Forum publications here:

<https://collaboration.opengroup.org/jericho/pages.php?pid=326&action=show&ggid=1633>

-
- ¹⁷ See Professor's Chadwick work here: <http://www.cs.kent.ac.uk/people/staff/dwc8/>
- ¹⁸ See: "Collaboration Oriented Architecture" http://www.opengroup.org/ericho/COA_v1.0.pdf
- ¹⁹ Carlos Trigos, "Required: Varieties of Identity to deliver the value of Cloud Computing," <http://carlos-trigos.com/2010/09/19/required-varieties-of-identity-to-deliver-the-value-of-cloud-computing/>
- ²⁰ Jay Galbraith, "Organizational Design: An Information Processing View," 1974
- ²¹ See also: Gartner, "Consider Identity and Access Management as a Process, not a Technology," 2005
- ²² R. Wang, D. Strong, "Beyond accuracy: What data quality means to data consumers," Journal of Management Information Systems, MIT, 1996
- ²³ See also: R. Y. Wang, H. B. Kon and S. E. Madnick, "Data Quality Requirements Analysis and Modeling," 1992
- ²⁴ See Donald Mitchell, Carol Coles and Robert Metz, "The 2,000 Percent Solution: Free Your Organization from "Stalled" Thinking to Achieve Exponential Success," 1999

5. Identity Services and Programme Delivery

Surveying the Landscape of Failure

This is perhaps the most difficult chapter of this book, not because of the theories involved, and also not because it reveals conceptual problems in the Security disciplines (which we have covered to some extent), but because it looks into the greater problem that is at the bottom - not of our thinking, but of our practice.

I refer to the delivery of IT and security solutions, at a project or portfolio level (IT programmes) where the problems I see are most relevant. The context is the interaction between the IT department experts and teams and the business units they work for. Here the IT teams and specialists are the service suppliers, and the business departments are the clients or consumers of the service. This distinction was not there all the time: the idea of the IT departments as suppliers of a service is itself the product of history, of the interaction with business processes and requirements along the last half of the 20th century. I think that the development of strong process-orientated doctrines as ITIL and BS7799 and COBIT all correspond to this experience, i.e. to a concerted effort to bring order and control to the interactions between the IT sphere and the business stakeholders and clients of IT.

Simultaneously we have seen the development and consolidation of pure project management disciplines like the PMP, PRINCE2, and others, and design and governance methods like TOGAF. All of this is obviously positive and signals a gradual maturation of the IT management-related practices. I have always encouraged their study, while at the same time cautioning about the proliferation of methods and tools, and also the incompleteness of some of these in respect to Security concerns. A greater concern though is that no matter how many of these methods are implanted and detailed, the history of IT project and programme delivery is a history of failure. To be more precise, this is a history of the “management of failure.”

There should be no confusion regarding what to expect or think of Project and Programme management, both in the public and private sectors. There are different drivers--“value for money” in the first case, and “profit” in the second--- but when it comes to IT initiatives, Programme and Project management are identical in their approach. In my experience, Security projects, including Identity management, are similar in this respect.

In a recent article in CIO Update, Jeff Monteforte¹ summarised the standard project approach very well: “At the most basic level, the objective of managing an IT project portfolio is performing a business case and return-on-investment (ROI) analysis for all proposed projects. Because the focus is on investment and return, the project portfolio governs and includes current and requested IT projects intended to improve or grow the business. [...] The desired result of maintaining a project portfolio is to align the technology investment funds, the IT resources, and the IT project work with organizational

business priorities. Each project is scrutinized for the ROI it can bring the organization, how it supports the current priorities of the company, and how much potential risk of failure is inherently associated with the project.”

All IT and Security managers and experts will recognise this approach, but also vouch for it, as we have learned in decades of work that there must be “alignment” with the business objectives. All the methods mentioned before are, in fact, ways to “align” IT with the project delivery process and the overarching organizational objectives. This certainly sounds obvious to everybody but why was and still is there a need for alignment? Is this a problem specific to IT? Has it been resolved?

To answer the first question, I believe that this is not a problem specific to IT or Security management in particular. It can be seen in all areas of technology as applied to business operations. The effort to “align” technology to organisational processes and value-driven controls is older and wider than those applied to IT. On the other hand, the results of this pressure towards alignment were particularly poor for decades and hence IT has stood out as a problem area. Perhaps this also explains the variety of methods and “standards” that have been developed to refocus IT in the mould of business and organisational objectives.

The problem has not been resolved, though, and this shows in the project failure statistics that are well known but rarely spoken about in our industry. Michael Krigsman quotes an interesting study by Geneca² in his ZDNET column³: “Most significantly, the report describes a highly negative situation in which most respondents expect their project to fail before it even starts!” For example, 78% of the respondents, out of a total of 596 business and IT professionals, believe that “the business” (code word for business management or business unit leads) is “usually or always out of sync” (meaning out of sync with the IT teams and experts). Krigsman highlights that 75% of the respondents “admit their projects are usually or always doomed from the start.”

“Doomed from the start” – a phrase that seems almost too harsh, and one that an objective observer may feel is not warranted – is nevertheless appropriate according to my experience across the IT professions and in Security and Identity management in particular. For example, in 2002 I made my own analysis⁴ of hundreds of Security projects in Europe while working for a major hardware and software vendor and found that over 70% of the software projects had experienced large delays leading in many cases to suspension or cancellation. To my surprise, only a small percentage of these problems were caused by software or hardware errors. The main cause of failure was generally “lack of alignment” between the business goals and the delivery of technical capabilities. I would not have seen Krigsman’s article as meaningful if it had not had relevance for my own experience, and I challenge any IT or Security specialist that may read this to deny that it is the case that we are swamped by project failures and lack of valuable results.

Personal experience—even if it is extensive-- or references, even if these are from keen and reputable observers of the Industry, like Krigsman, can be disputed by questioning the definition of project failure- for example by asserting that a project is not a failure if the project manager or the business

unit cut it short just in time to avoid losses. Some diversion is also caused by the notion that business should tend to “fail fast” in a trial and error process, while progressing towards some target. All of that is fine and makes sense if you move within the rules of the permanent conflict between “the business” and “IT” - that is, if you accept that there is a gap, and that it is perhaps the mission of the Programme and or Project manager to cut the wings of some incurable IT technologists who want to spend money without end.

Is this a realistic picture of what is happening? Programme and Project managers are somehow heroic business-orientated people who stop the abuses of so many IT dreamers? Or, is it the case that, as we say in our profession: “the business does not ‘get’ technology.” My answer is that there is no innocent party in this case, and that both those who ‘get’ IT and those who don’t are complementary actors in the story. In other words, the misalignment is real. The reader should remember that everything that is applicable information technologies is also valid for Security and Identity management, with special characteristics that I will highlight towards the end of this analysis.

Decade after decade we have seen statistics showing the problems in IT delivery. Some of the older sources, like the 1995 Chaos Report⁵ (Standish Group), reveal 31.1% of projects will be cancelled before they get completed, and 52.7% of projects will cost over 189% of the original estimates. These figures have been criticised by academics and industry experts. For example Laurenz Eveleens and Chris Verhoef⁶, of Vrije Universiteit (Amsterdam) reject the classification and estimation assumptions of the 1994⁷ Chaos survey which “reported a shocking 16% project success rate, another 53% of the projects were challenged, and 31% failed outright.” It is important to note that these figures (as all the Chaos report statistics) refer to software implementations. The authors challenge the report’s definitions of successful, challenged and impaired projects.

Eveleens and Verhoef write: “[...] Standish defines a project as a success based on how well it did with respect to its original estimates of the amount of cost, time, and functionality. Therefore, the Standish “successful” and “challenged” definitions are equivalent to the following: Resolution Type 1, or project success. The project is completed, the forecast to actual ratios (f/a) of cost and time are ≥ 1 , and the f/a ratio of the amount of functionality is ≤ 1 . Resolution Type 2 or project challenged. The project is completed and operational, but $f/a < 1$ for cost and time and $f/a > 1$ for the amount of functionality.”⁸

This challenge is justified, as we would also expect that the success or failure definitions could handle all possible cases, including those where the project is within budget but is nevertheless “challenged” in terms of functionality. Regrettably the study by Eveleens and Verhoef shows its own limitations when they declare: “In reality, the part of a project’s success that’s related to estimation deviation is highly context-dependent. In some contexts, 25% estimation error does no harm and doesn’t impact what we would normally consider project success. In other contexts, only 5% overrun would cause much harm and make the project challenged. In that sense, there’s no way around including more context (or totally different definitions) when assessing successful and challenged projects. However, the Standish definitions don’t consider a software development project’s context, such as usefulness, profit, and user satisfaction.”

That, sadly, leads the researchers into a peculiar path of trying to determine “forecast bias” and trying to assess factors that correct the bias in the forecast, by which then they obtain lesser failure rates. This is not what we, the IT and Security practitioners would consider a good approach to replace the original Standish reports; it even reveals that probably many organisations are “forecasting” delivery costs inaccurately! At the same time, what do we make of a project where the costs have a 25% deviation? Should we consider a 15% deviation as “best in class” as the authors suggest?⁹ Yes, more “context” is necessary, but the lack of appropriate measures for “usefulness, profit and user satisfaction” is an obstacle, and this has not been addressed by this study or other critics of the Standish Group work and similar reports. How are the Programme and Project managers going to address usefulness and satisfaction if it is not backed by standard, organisational quality controls, as there is no universal quality measurement? How do we measure for example an Identity management solution? Does it contribute to user satisfaction or should we focus on data availability? How are the programme and project managers going to judge delivery costs if not by numerical comparison of cost projection and aggregated real costs? Organisations may differ in their cost forecasting methodologies, but is it not always the case that there are organisational biases in forecasting that can’t be reduced to some standard?

So when we read estimates or judge our own experience in respect to project success we are not doing a mathematical calculation but a subjective judgement, already specific to the context (i.e. the organisation being considered) and not trying to formulate a general law. In reality, the Standish Group and other organisations have done a great service in focusing attention to poor results in project delivery. While other researchers’ results are different in the detail, the overall difficult and concerning situation is the same.

People should certainly be careful when quoting the Chaos report or similar studies, considering that these are mostly surveys or based on limited samples of the IT industry project landscape. It should also be clear that we are seeing aggregate data, and very different questionnaire techniques which may not lead to “scientific” results, but it is also true that almost any survey and any study of this matter brings up alarming results, and this after decades of development of the methods supposedly driven to avoid this kind of failure. In this respect, the words credited to Martin Cobb, Chief Information Officer of the Branch Treasury Board of Canada Secretariat, still stand unchallenged: “We know why projects fail; we know how to prevent their failure, so why do they still fail?”¹⁰ Moreover, there are many other sources that point in the same direction. Let’s look at some here:

- A study by Dr John McManus and Dr Trevor Wood-Harper of the British Computer Society covering years 1998-2005 and 214 information systems development projects in Europe found that only one in ten projects could be considered successful, i.e. not over budget or unable to deliver required functionality.¹¹
- Joe Harley, the Chief Information Officer at the Department for Work and Pensions (UK), revealed that “only 30%” of technology-based projects and programmes are a success - at a time when taxes are funding a £14bn spend annually on public sector IT.¹²

- A KPMG study in 2005 showed that “A quarter of the benefits of IT projects are being lost by organisations across the globe because of management failures during a project’s lifecycle [...] KPMG International's survey of 600 organisations across 22 countries revealed that 86% of respondents reported the loss of up to a quarter of their targeted benefits across their project portfolios. Nearly half of respondents reported at least one project failure in the past year, an improvement from KPMG’s 2003 survey where 57% experienced one or more project failures in the previous 12 months.”¹³ This reference is relevant as KPMG reports that success is being defined in terms of business benefits delivery instead of using only time and budget parameters.
- Chris Sauer, Andrew Gemino, and Blaize Horner Reich found that one third of IT projects fail.¹⁴ The researchers interviewed project managers, instead of business executives, as the Chaos Report did, leading to different failure rates overall. The authors write: “Surprisingly, we found that one-quarter of projects underperform however small their size. Even projects with budget less than £50,000, effort less than 24 person-months, duration shorter than six months, or team size of less than five experienced 25% risk. There is a significant level of risk regardless of size.”
- A study of 100 Fortune 500 companies by Keith Ellis, IAG Consulting,¹⁵ in 2008, notes that “68% of companies are more likely to have a marginal project or outright failure than a success due to the way they approach business analysis. In fact, 50% of this group’s projects were “runaways” which had any 2 of: taking over 180% of target time to deliver; consuming in excess of 160% of estimated budget; or delivering under 70% of the target required functionality.”
- Scott Ambler, writing about a sample of 203 projects in Dr Dobb’s Journal, states that “According to the 2010 IT Project Success Survey, our success rates are: Ad-hoc projects: 49% are successful, 37% are challenged, and 14% are failures. Iterative projects: 61% are successful, 28% are challenged, and 11% are failures. Agile projects: 60% are successful, 28% are challenged, and 12% are failures. Traditional projects: 47% are successful, 36% are challenged, and 17% are failures.”¹⁶ It is important to note that Ambler’s focus is strictly on software development projects.

These are only some examples of a vast number of sources of very different theme and quality, but all pointing in the same direction discussed here: it can be asserted with great certainty that the status of programme and project delivery is problematic and requires further investigation.¹⁷

Above all, considering the variability between sources, the limitations of the surveys in size and quality, and the diversity of areas covered, it is decisive to focus on the types of problems detected. In other words, while it will be very difficult to get a complete quantitative understanding of the problem, or a common measuring technique, we can have a view of the common causes of programme and project failure.

The Causes of Failure

Perhaps the best summary of these causes was published by the British Computer Society in the study cited above.¹⁸ Their classification is very detailed, so we will centre our attention on the “key reasons” for project cancellation:

- Business strategy superseded
- Business processes change (poor alignment)
- Poor requirements management

- Business benefits not clearly communicated or overstated
- Failure of parent company to deliver
- Governance issues within the contract
- Higher cost of capital
- Inability to provide investment capital
- Inappropriate disaster recovery
- Misuse of financial resources
- Overspends in excess of agreed budgets
- Poor project board composition
- Take-over of client firm
- Too big a project portfolio

Together with these factors, the authors of the BCS study also list management and technical reasons, among others the following:

- Ability to adapt to new resource combinations
- Differences between management and client
- Inappropriate architecture
- Inappropriate coding language
- Inappropriate technical methodologies
- Inappropriate testing tools
- Insufficient domain knowledge
- Insufficient end-user management
- Insufficient reuse of existing technical objects
- Insufficient risk management
- Insufficient software metrics
- Insufficient training of users
- Lack of formal technical standards
- Lack of technical innovation (obsolescence)
- Misstatement of technical risk
- Obsolescence of technology

In the whole, McManus and Harper seem justified in writing in their conclusions a harsh assessment of the situation: “On examination of the project stage reports it became apparent that many project managers plan for failure rather than success. If we consider the inherent complexity of risk associated with software project delivery it is not too surprising that only a small number of projects are delivered to the original time, cost, and quality requirements. Our evidence suggests that the culture within many organisations is often such that leadership, stakeholder and risk management issues are not factored into projects early on and in many instances cannot formally be written down for political reasons and are rarely discussed openly at project board or steering group meetings although they may be discussed at length behind closed doors.[...]One of the major weaknesses uncovered during the analysis was the total reliance placed on project and development methodologies. One explanation for the reliance on methodology is the absence of leadership within the delivery process.”¹⁹ Let’s see other classifications that are equally relevant. In a study by PM Solutions,²⁰ the researchers found that the main causes of failure were:

- Unclear requirements, lack of agreement, lack of priority, contradictory, ambiguous or imprecisely defined
- Lack of resources, resource conflicts, turnover of key resources, and poor planning
- Tight schedules, unrealistic and overly optimistic goals
- Planning based on insufficient data, missing items, insufficient details, and poor estimates
- Unidentified risks, assumed but not managed

Overall, I find that this list precisely suggests the type of problems indicated in the BCS study, hinging on lack of business (not IT) leadership of the delivery process. If we judge this by the more or less standard success criteria defined by J. Kent Crawford²¹ in his book *The Strategic Project Office*,²² we have a better grasp of what is going wrong as we could rewrite these criteria for a large number of organisations as follows:

- The organisation's strategies are not executed according to plan
- The organisation's shareholders are not satisfied with the IT investment/benefit ratio
- A large percentage of the IT projects are not completed on schedule and on budget
- The IT project internal clients are not satisfied
- Project resources are not allocated optimally
- IT projects are not aligned to the organisation's business strategies
- The organisation does not work on the right IT projects in a significant number of cases

In essence, my point is that we are looking neither at IT or Programme Management failures. As the BCS study says, actually we are seeing an excessive reliance on "management processes" if not even "anticipation of failure." On the side of IT, we know that it is not a matter of refusing alignment with the business, a goal that is now very entrenched in every segment of the IT professions. Contrary to this, frustration in the IT and expert teams stems from a general lack of communication and leadership at an organisational level.

The Office of Government Commerce (OGC, UK) has summarised the causes of project failure as follows, pointing again to issues rooted in lack of leadership and failed business and IT alignment:²³

- Lack of clear link between the project and the organisation's key strategic priorities, including agreed measures of success.
- Lack of clear senior management and Ministerial ownership and leadership.
- Lack of effective engagement with stakeholders.
- Lack of skills and proven approach to project management and risk management.
- Too little attention to breaking development and implementation into manageable steps.
- Evaluation of proposals driven by initial price rather than long-term value for money (especially securing delivery of business benefits).
- Lack of understanding of and contact with the supply industry at senior levels in the organisation.
- Lack of effective project team integration between clients, the supplier team and the supply chain.

In other words, IT Programme and Project failures are organisational failures not peculiar to the IT areas themselves, but more prevalent in these. Although this discussion has taken many pages, I think it was necessary to set the stage for what follows.

IT and Information Security as Business Sub-Systems

I believe that nobody would be surprised if I said that the explanation of these issues lies in seeing IT -- and IT Security within it--- as a sub-system of the organisation. This must be refined and explained to understand that the term sub-system does not mean here that IT is “part” of the organisation. I go further in saying that IT security is not part of IT either, and this requires even more explanation.

As I wrote in previous chapters, Identity management is dependent on Security initiatives; Security, in turn, is dependent on IT and IT is dependent on Business programmes, but being dependent on something does not mean “being part of it.” Strictly a part of a whole implies some form of inclusion, while my contention is that neither IT nor IT Security are “part” of the business in this sense. In other words, these are not included in business models or operations. In my view, IT operations are a sub-system only in the sense that our processes and activities are coupled or linked to business operations, but both realms are self-contained and are different communication systems.

Not only the conceptual differentiations of one and the other system are separate, but there is in fact no common language across the boundary between these two areas. Even more, if we look into the IT departments themselves, we will see various sub-disciplines that do not share the same distinctions and conceptual frameworks. I put special emphasis on Security and Identity but it is clear to me that other areas can be equally investigated as having a closed language and specific self-referring processes which are foreign to the other areas in the organisation.

It would be an error to consider that this state is the product of some confusion or lack of understanding. Quite the contrary, most of the issues revealed in the failure statistics can be seen as inevitable effects of the interaction of these separate, self-contained sub-systems. Either when the exasperated IT experts declare that the business does not ‘get’ technology or when the business lead stops listening to an IT department that does not ‘get’ the business goals, what we should see there is not a failure in communication, but the normal state of communication between these parties. This “normal” state is generally one of “hostile cooperation” and lack of common goals.

As Will McWhinney²⁴ explains, we (the organisation’s actors) create a large part of our problems and issues in the act of trying to resolve them, and our efforts yield unintentional results. I think that this is meaningful in more than one sense. For example, a deeper understanding of the permanent misalignment of IT and Business would lead to new success criteria, where a solution would be measured by the degree “in which it frees the organisation from one or another side of the dilemma it does not create new problems,” according to McWhinney.

This is insightful, because problems are solved with resources (as every programme manager knows), but then the attempts to solve problems involving teams and individuals who hold different world-views leads to new problems. So for example the adoption of IT technologies in organisations, initially

intended to solve administrative or production problems, in all cases leads to new unexpected issues across the organisation. It is not as the techno-optimist would say that the systems were not properly designed or were delivered late, but that the systems could not be delivered much better in any case.

This is not a pessimistic view though. Excellent delivery is possible but it will be the exception, not the rule. At the basis of this understanding is the notion that every aspect of an organisation is contingent (i.e. not necessary or predetermined), but dependent on the correlations between the organisational actors, as shown by the German sociologist Niklas Luhmann.²⁵

The attempt to solve a problem involving people who hold different perspectives creates new problems, as McWhinney says, and the organisation becomes a self-generator of problems. The contingencies of human organisations and communication sub-systems become inevitabilities of conflict and failure. It is not true that projects are “doomed to failure” from the beginning, but it is true that most IT projects will fail or deliver the wrong solution at the wrong cost and at the wrong time.

Looking towards other areas of the organisation, we can see that there are also inevitable frictions between its sub-systems and the “external” consultancy organisations that are hired to support various activities. This is a critical point of the systemic view of the organisation. In the same way as individuals are not “part” of societies (in the Luhmannian sense), they are also not part of other sociality levels, i.e. “lower” levels of human organisation and communication structures between individuals and groups.

Between these units, each of which has an “operational closure,” there is no transfer of meaning or “information flow.” As a consequence of this discontinuity, there is a need for paradoxical action and the use of interactions or “couplings.” It is this we should seek when aiming at excellence in delivery, and not just compliance with specified processes. In other words, excellence is achieved through the contradictions in the organisation, and not through the elimination of these contradictions.

In the terms that I have been proposing for the articulation of Security programmes, excellence in delivery is achieved through the correlation and contraposition of disparate but complementary goals of each of the perspectives: Direction, Selection, Protection and Verification. Here, the role of the business which I labelled as the “missing discourse” in Chapter 1 pertains to the perspective of Direction. It is therefore essential to assume as a fact that the disciplines of Direction are contradictory with those of protection (generally aligned with the techno-centric emphasis of the IT departments).

Ultimately the cause of these contradictions is none other than the constant progress of division of labour within the organisation, which is itself a product of capitalistic development at economic and social levels. These differences within differences are specialisations of groups and opinions (which I call “perspectives”), and consist of logical derivatives of communication sub-systems within the organisation. This allows us to understand too that periods of rapid change such as the one we live in, with the continuous adoption of technologies by business organisations, create a permanently unstable ground. Business seeks mobility, investment agility, cost reductions, globalisation of markets, and in this context they test and adopt any mechanism, any technology that may enable some advantage in the market. Not all technologies succeed in this sense, and also competitors adopt the

same differentiators successively reducing the initial advantage. In this way, the cycle of technology adoption –leading now towards IT outsourcing and cloud-based computing—does not settle down.

New technologies also suit an increased, in many cases global, mobility of personnel and consumers. All of which leaves the IT organisations behind, always chasing the next move by the business. Can IT deliver? Can IT be secure in this context? In everything we have covered in this chapter we find multiple circles of causes and effects that superficially look like a tendency towards failure in IT Programme and Project delivery, but are really an inevitable consequence of the bounded interaction, the contradictions between the various sub-systems of the organisation. These contradictions show in paradoxical results, when the IT departments “fail to deliver” or when IT security creates new probabilities for insecure information management by opening more and more channels in the desperate attempt to “serve the business.”

Security and Identity Investment Decisions

If we review retrospectively the IT press for the past two decades, we see how opinions have changed. What was the main problem being discussed in IT Security in 1995? What was the main solution? If we focus on investment levels for example, we notice that for about half that period the predominant opinion was that the Security investment levels were too low. In the second half the opinions tended to be IT investment levels were rising quite fast and probably were reaching a plateau. There were the usual alerts about small and medium-sized organisations where Security investment was deemed still to be too low, but the consensus was that large organisations were spending between 8 and 12 per cent of their IT budgets in Information Security.

Paul Strassman,²⁶ a long-time researcher in IT security from the point of view of corporate management, even alerted his readers that exceeding 10 per cent of the IT budget might indicate poor investment criteria and bad results. Along the period reviewed, there was a consistent effort from the side of the industry and even academia to substantiate investment in security. It seems to me that this effort was successful in demonstrating that investment levels were “too high” by focusing on showing problems in the “return” of Security investments. Several theories arose, but the dominant one was the so-called “risk-based security investment analysis,” which I have discussed in previous chapters.

It is almost impossible to find a critical view of risk-based analysis, outside of the works by Donn Parker,²⁷ Gurpreet Singh Dhillon,²⁸ and James Backhouse.²⁹ Nevertheless, the dominance of risk-based Security –which corresponds to the prevalent techno-centric perspective – is not absolute, and along the entire period it is possible to find other paradigms at play. This has been shown by Dr. Elspeth McFadzean, Dr. Jean-Noël Ezingear, and Professor David Birchall³⁰ in an important study on research paradigms in Security and Governance. The authors use the well-known Burrell-Morgan paradigmatic model which has been very successful in Sociological research.³¹

I am concerned here with the dominant paradigm, which I classify as “mechanistic,” not because I seek a “paradigm shift” from this towards any of the other fundamental perspectives, but because I want to promote competition and co-operation of the four key Root Metaphors (in the terminology of Stephen

C. Pepper). It is my opinion that the lack of balance, competition and cooperation, the deeply-rooted presumption that the only mechanism is a valid computer science and information technology approach, has had a harmful effect on our profession and all types of organisations.

Once we move away from the idealistic conceptions that seek some form of pure “communication” between the various aspects of the business and understand that each paradigm is represented by a closed sub-system as explained in previous sections, we have more chances of achieving solutions that represent the correlated interests of these groups and tendencies. It would be a benign assumption that these perspectives should be purposefully combined; avoiding for example the unilateral sway of the techno-centric Security “Protection” approaches; but this would not be realistic. A better take on this matter recommends a combination of cooperation and competition, and hopefully not “hostile cooperation” which is the status we have now.

In an extreme form without competition and control from the other perspectives, any one of them degenerates into a formula, a fragmented view of reality that is not capable of holding the organisation together. For example, the mechanistic paradigm in security will insist on “protecting information assets” and “establishing a perimeter protection” around these, when the other tendencies of the organisation call for wider circulation of information and do not operate within “perimeters” anymore. On its side, the “Direction” perspective, unable to compete and cooperate with the others, will continuously miss investment opportunities, thereby producing the usual silo-orientated approach that we see in so many organisations where each business unit operates almost a private IT environment.

We have seen already how risk-based Security has serious limitations, but we can add to these even more. A key one is that risk-analysis cannot be extended to the whole organisation. Consider for example how difficult it would be to blend into one risk framework valid Security issues as different as compliance (associated to the Verification perspective), user access control (pertaining to the Selection perspective), and trust management (addressed by the Direction perspective). If even within the “attack and defence” logic of the mechanistic paradigm it is impossible to calculate objective probabilities, consider the meaninglessness of trying to “calculate” risk values for a combination of the four fundamental paradigms at play in organisations.

This has immediate relevance for Programme and Project delivery as it refers to the notions of alignment and business objectives. Information security expenditures can be considered as being part of business investments when they enable processes, when they help complete value chains, open markets, deliver services and goods; but seen from a different perspective, they are operational expenditures and similar to building maintenance or office overhead outlays. A detailed analysis of any Security investment rapidly leads to seeing them as having multiple direct and indirect, as well as financial and non-financial, results or “impacts.”³²

	Financial	Operational
Direct	By directly reducing costs and project effort • IT cost reduction • Infrastructure simplification • Shared Service Strategy • Project cost reduction • Smaller user mgmt. team • Less access mgmt.costs • Less Audit Fees	By protecting business assets • Compliance • Data Protection • Financial Market Rules • "Need to Know" Principle • Audit Issues • Access Governance
Indirect	By indirectly enabling business processes • Business Process agility • Joiners, Movers, Leavers mgt. • Directory Integration • HR integration • IT Streamlining • Self Service PW reset	By improving staff and partner productivity • User productivity • New products • Partners and services integration • Product Planning security • Accountability • Control enhancement

Four classes of benefits of Identity Management solutions

Therefore Security programmes and expenditures contribute to the overall returns on capital allocations, but there is no ROI or “return on investment” for Security allocations per se. It is still fashionable to speak about ROI on Security as experts try to adopt and mimic the “language of business,” but this is a fruitless effort to date. This is only the product of our training, whereby we have learned that we have to be aligned with the business leadership and teams, but we fail because we adopt that language while still talking to ourselves and see only the side of risk avoidance (i.e. protection) and ignore the risk-taking side, which is the realm of Direction and the discourse of the Master.

For sure, there are some important interpretations of this, more or less useful for project financial justifications, but this falls into the trap of positioning Security again as expenditure, a pure cost, unrelated to the business and aiming at most at some cost-savings or cost avoidance. From the strict point of view of capitalist microeconomics it is not possible to derive capital returns from Security expenditures. Hence Programme and Project management will operate “by the book,” “align with the business” and still deliver poor results. Or, as the BCS report remarked: “manage for failure.” Helping to compose the problem, the IT and Security experts will happily sign off the project deliverables, without knowing what value is being delivered for the organisation, insisting, as we always do, on the mechanistic protection of “information assets” - but these have no value unless they are trusted to others and not only “protected.” The effect of these misunderstandings and obscure “collaboration” in failure is enormous, as it settles the organisation in year after year of dreary routines and underachieving teams.

The Value of IT

Matt E. Thatcher and David E. Pingry describe the current situation as follows:³³ "Although profit-seeking firms continue to invest in information technology (IT), the results of the empirical search for IT

value have been bafflingly mixed --leading Nicholas Carr and other leading pundits to argue that IT has become a commodity input that, from a strategic standpoint, doesn't matter." According to Carr, "It remains difficult if not impossible to draw any broad conclusions about IT's effect on the competitiveness and profitability of individual businesses... companies continue to make IT investments in the dark, without a clear conceptual understanding of the ultimate strategic and financial impact."³⁴ This is one more indication of how different reality looks when seen by people who research the industry as a whole and how practitioners see the things from the "inside."

Thatcher and Pingry study IT investment with a strange differentiation between "design tools" and "production tools." I believe that this subdivision comes from an overestimation of the software development industry model. More important is that they compare results of investments considering monopolistic and competitive markets, digital products and traditional products, and conventional measurements of costs and profitability. Thatcher and Pingry show that in a competitive market, even if IT investment directly improves the cost efficiency of a firm, the business value "as measured by profits, productivity, and consumer value [...] is constrained by the market structure." In other words, in a context where IT and all related investments are becoming a commodity input, the "benefits" generated by these areas can be estimated only --if at all--in the context of the general profitability of the business or organisation.

Thatcher and Pingry write: "In the absence of collusive behaviour the firms will compete in product quality improvements but will be less able to gain competitive advantage and improve profitability. In fact, given that IT is a commodity available to all firms, firms are compelled by strategic necessity to compete in product quality improvements in this case. According to Clemons,³⁵ the idea behind strategic necessity is that "instead of becoming a source of lasting competitive edge, most strategic information systems become new and essential aspects of doing business... that is, profits will be competed away. Since the key resources of management information systems (MIS) applications are commodities available to all competitors, all competitors with similar MIS strategies can develop similar systems and benefits such as reduced costs or improved service."

And they conclude: "The major objective of individual businesses is to generate profits by reducing production costs, improving product quality, improving firm productivity, and increasing consumer value. Much of the IT literature is focused on empirically examining ways IT investments may accomplish these goals. However, while it may be necessary for firms to pursue IT investments due to competitive pressures, strategic necessity, or firm survival, our work demonstrates these same IT investments may not result in improvements in traditional measures of business value. Our work adopts the view of IT as a commodity input where investment in IT does not, in and of itself, create a market advantage for any one firm."³⁶

I believe that this research supports my suggestion to look at the interplay of all the factors in the organisation and stop searching for a "return" of investment of security. A well-informed business leader will only laugh at the suggestion that a particular technology will bring some "benefits" in and by itself; but also we should laugh at the views that this opens, when we see that so many IT and

Security projects are cancelled we will understand why this happens and not complain absurdly that the business does not ‘get’ technology. In fact, what we call “the business” or “management” definitely understands that technology is either an instrument of capital, or it is not, even at the expense of any Security.

Identity Programmes and Projects

Identity management falls into this context obviously on the side of IT itself. Nevertheless, it does so in an even more contrived position than other segments of the technology services. This is because Identity management is the least technological of all these specialities and the one that impacts more business activities more directly. As I will show in later chapters, Identity management solutions cover all forms of benefits and impacts in an organisation: direct and indirect, financial and non-financial. It is particularly important to see that none of the other investments in technology reach completion with an input of the Identity management disciplines. Either in terms of access control or user enablement, there is an essential relationship between the technology itself and the user of the technology. A technology only delivers value if it is exploited by direct and indirect users, inside and outside the organisation.

Hence the importance of Identity management for any Programme and Project in all types of organisations. The problem is though, that this relevance is not reflected in how Identity management is delivered at present. What I have seen in hundreds of projects across Europe in the past 13 years is a vast landscape not of “failed” projects (as other IT experts may want to recognise), but a vast lack of Identity management projects. In other words, Identity management is absent from all major IT transformation programmes and initiatives. It is not the case that there are failed Identity projects. There are many, but there are more programmes that just don’t have this component. If we used my perspective model to describe the situation, we would say that these Programmes and Projects lack the Selection perspective.

Identity management requires an enterprise-wide focus so that it can interact adequately with the rest of the organisation. The Identity management solutions must be based on a “circle of trust” encompassing the four perspectives discussed in several parts of this book. These, as the reader may recall, correspond to the disciplines of Direction (Trust Definition), Selection (Trust Allocation), Protection (Trust Enforcement) and Verification (Trust Monitoring). In this framework, the Identity management domain has to be conceived in terms of Trust Allocation and based on the Selection disciplines (also called “trust establishment” in my work). For this reason, every IT Programme and Project should specify tasks and ownership for these areas, considering these as foundational disciplines for the rest of the Security areas of concern. We will see in the next few chapters how Identity management needs to adopt a quantitative method to obtain an appropriate place in the organisation.

-
- ¹ J. Monteforte, "De-Mystifying PortfolioManagement" ,
<http://www.cioupdate.com/print/insights/article.php/3432721/De-Mystifying-Portfolio-Management.htm>
- ² <http://geneca.com> and <http://www.genecaresearchreports.com/index.html>
- ³ Michael Krigsman, <http://www.zdnet.com/blog/projectfailures/research-75-percent-believe-it-projects-are-doomed/13016>
- ⁴ Carlos Trigos. *A call for Level 4*, IBM Corporation internal communication, 2002
- ⁵ Chaos Report, Standish Group, 1995
- ⁶ L. Eveleens and C. Verhoef , "The Rise and Fall of the Chaos Report Figures," IEEE Software magazine, 2010
- ⁷ Chaos Report, Standish Group, 1994
- ⁸ Laurenz Eveleens and Chris Verhoef , "The Rise and Fall of the Chaos Report Figures," IEEE Software magazine 2010
- ⁹ Laurenz Eveleens and Chris Verhoef, "The Rise and Fall of the Chaos Report Figures," IEEE Software magazine 2010. See also: <http://www.guerrillaprojectmanager.com/the-chaos-report-myth-busters>
- ¹⁰ Martin Cobb, (1996). "Unfinished Voyages: a follow-up to the CHAOS Report," Standish Group Report, http://www.standishgroup.com/sample_research/unfinished_voyages_1.php
- ¹¹ J. McManus and T. Wood-Harper "A study in project failure," <http://www.bcs.org/content/ConWebDoc/19584>
- ¹² Cited by Ted Ritter in "Public sector IT projects have only 30% success rate," <http://www.computerweekly.com/blogs/public-sector/2007/05/public-sector-it-projects-have.html>
- ¹³ Cited by Katharine Hollaway in "KPMG highlights IT project failures," 2005 ,
<http://www.accountancyage.com/aa/news/1769596/kpmg-highlights-it-project-failures>
- ¹⁴ Chris Sauer, Andrew Gemino, and Blaize Horner Reich. "The impact of size and volatility on IT project performance," 2007
- ¹⁵ K. Ellis, "The Impact of Business Requirements on the Success of Technology Projects," IAG report, 2008
- ¹⁶ Scott Ambler citing results of his research in
<http://www.drdoobs.com/article/print?articleId=226500046&siteSectionName=architecture-and-design>
- ¹⁷ Additional sources:
http://www.theregister.co.uk/2002/11/26/it_project_failure_is_rampant/print.html
[http://www.it-cortex.com/Stat_Failure_Cause.htm#The%20Bull%20Survey%20\(1998\)](http://www.it-cortex.com/Stat_Failure_Cause.htm#The%20Bull%20Survey%20(1998))
- ¹⁸ J. McManus and T. Wood-Harper "A study in project failure," <http://www.bcs.org/content/ConWebDoc/19584>
- ¹⁹ J. McManus and T. Wood-Harper "A study in project failure," <http://www.bcs.org/content/ConWebDoc/19584>,
- ²⁰ Cited by M. Krigsman : <http://www.zdnet.com/blog/projectfailures/cio-analysis-why-37-percent-of-projects-fail/12565>>
- ²¹ J. Kent Crawford's page at PMSolutions: <http://www.pmsolutions.com/blog/authors/j-kent-crawford/>
- ²² J. Kent Crawford. *The Strategic Project Office*, CRC Press. 2010. Crawford's criteria are:
- The organization's strategies are executed according to plan.
 - The organization's shareholders are satisfied.
 - The organization is financially successful.
 - Projects are completed on schedule and on budget.
 - Project customers are satisfied.
 - Project resources are allocated optimally.
 - Projects are aligned to the organization's business strategy.
 - The organization works on the right projects
- ²³ NAO-OGC "Common Causes of Project Failure," <http://www.dfpni.gov.uk/cpd-coe-ogcnaolessons-common-causes-of-project-failure.pdf>
- ²⁴ W. McWhinney, "Paths of Change: Strategic Choices for Organizations and Society," 1992.
- ²⁵ Niklas Luhmann, "Soziale Systeme," 1987
- ²⁶ Paul A. Strassman, "The Business Value of Computers," Information Economics Press, 1990
- ²⁷ D. B. Parker, "Fighting Computer Crime: A New Framework for Protecting Information," 1998
- ²⁸ G. A. Dhillon, "Interpreting the Management of Information Systems Security," University of London, 1995
- ²⁹ J. Backhouse and G. Dhillon, "Structures of responsibility and security of information systems," European Journal of Information Systems, 1996
- ³⁰ Dr. Elspeth McFadzean, Dr. Jean-Noël Ezingard and Professor David Birchall, "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," Henley Management College, 2004. <http://www.information-institute.org/security/3rdConf/Proceedings/9.pdf>
- ³¹ G. Burrell and Gareth Morgan, "Sociological Paradigms and Organizational Analysis," 1979
- ³² I use this image when explaining the need for quantitative and qualitative measures of the value of Identity management.

-
- ³³ Matt E. Thatcher and David E. Pingry, "Modeling the IT Value Paradox," Communications of the ACM, August 2007
- ³⁴ Nicholas Carr. *IT doesn't matter*. Harvard Business Review, May 2003 and Nicholas Carr, "Does IT Matter? Information Technology and the Corrosion of Competitive Advantage, Harvard School Press, 2004
- ³⁵ E. Clemons, "Strategic necessities," ComputerWorld, 1988
- ³⁶ Matt E. Thatcher and David E. Pingry, "Modeling the IT Value Paradox," Communications of the ACM, August 2007

6. The Cloud Transforms the Network

Identity in the Cloud

The rise of Cloud Computing in the recent past is history repeating itself. This is often the case in the technology markets, where old concepts reappear wrapped in funny names and marketing campaigns. In the case of Cloud Computing, even the shallowest research shows the continuity of the model since the “era” of the mainframes, “computing on demand” and the almost-forgotten “the network is the computer” period.

It is evident the combination of virtualisation, hosting, web services, new security protocols, outsourcing, performance enhancements and other infrastructural capabilities has created a new panorama in our business, but how new is the Cloud really?

It is impossible to ignore that various business sectors are moving rapidly to streamline their IT services by outsourcing all capabilities that can be acquired as utilities in the market. From data storage to off-the-shelf accountancy applications, firewalls and application monitoring, it has become simple, practical and advantageous to use remotely hosted, managed services.¹ The expansion of Cloud computing is equally fast in the public sector.²

But the novelty of these changes should not obscure the fact that Cloud-like capabilities have existed since early in the Computing Era, as remote, scalable, virtual, shared, resilient server resources were always at the core of major corporate and governmental IT infrastructures. While in the past these capabilities were almost exclusively mainframe-based and mostly used by large organisations, now they are widely accessible and not restricted to a single type of technology. Their evolution has consisted not in the disappearance of the original platforms, but in the combination of many more platforms and layers of systems alongside or “on top” of the earlier ones. More critically, individual use of remote capabilities has also become a fact of life.

This can be formulated as follows: The history of IT technologies in all areas of business, government and daily life advances by multiplying the levels of indirection, the “tiers” of the environment. This is the case in software engineering as well as in hardware systems. A good outline of this progression is captured in the maturity layers described by the Service Oriented Architecture (SOA) discipline:³

- A) Silo
- B) Integrated
- C) Componentised
- D) Services
- E) Composite
- F) Virtualised
- G) Reconfigurable

When using these categories, it is important to recognise later stages do not replace the earlier ones but combine with them. In fact, today all these layers and steps of the technological world coexist. Technological evolution increases complexity.

This is relevant when we work in socio-technical environments (corporations, organisations) where there is a high component of “legacy” platforms and applications, representing the earlier stages of technology. To address the relationships between the various segments and levels of maturity of the organisation, it is essential to use an SOA approach.

Today, we see organisations collaborating and exchanging information “in the Cloud” but that does not mean they have abandoned their corporate infrastructures altogether, and it is safe to predict that Cloud adoption will be uneven across sectors and geographies. On the other hand, even the most “backward” organisations will adopt at least partial “Cloud” services and use either federated or corporate Identity management models to enable user access across their boundaries. A key contribution to this understanding is the work by a number of experts associated with the Jericho Forum.⁴

Does the current situation lead to an “end of corporate Identity management”? As we analyse case after case of organisational environments, we see that cloud-based solutions will tend to grow in parallel to the traditional business processes. Data governance, for example, remains as a process closely guarded by organisations. What this means is the Cloud phenomenon transforms the network, by making it more complex and large, while public and private organisations retain past levels of complexity and control. The increase in complexity precisely reflects the continued existence of internal, “in house” processes and technologies.⁵

The technologies and models underpinning the “Cloud” trend are not new, but the general application of these trends is. The main change, easily forgotten when discussing the Cloud, is not in the technology but in the modalities of access and use of technology. In other words, what matters the most is the range and variety of users “in the Cloud.” This fact should be enough to propel the Security and Access Management principles to the centre of the discussion, but that has not happened. On the contrary, Security has become a blocking factor instead of a supporting discipline because of the lack of understanding that persists in this respect.

From the perspective of standard, Protection-focused Security, the problems of user access in the Cloud are the same as those catalogued for the earlier period. Seemingly, nothing has changed. The emphasis on “protecting information” is simply translated to wider and more complex environments across the Internet. Instead, from the perspective of “Direction” and “Selection,” which I want to highlight in this book, the problems of user access have changed fundamentally. We still have to face the issues experienced in a traditional “closed” enterprise environment, and we still have to resolve the problems of managing user access to legacy applications, but now we are facing challenges related to the propagation of identities inside and outside of the organisational boundaries. These problems

did not exist before. Organisations have moved into “boundary-less” computing, but also into an environment where they interact with suppliers, competitors, contractors, service providers and other organisations on a peer-to-peer basis.

The authentication and authorisation of users moving across the network has become a problem in this sense, because organisations do not own all the sources of identity data, and, instead, have less and less control over user and data movements as the trend continues. It is very important to see here the driving force of change was and is not the technology of the Cloud, or computing technologies in general, but the evolution of organisational and business models of action in the economy and society. Computers and networks enable the change, but they don’t create it.

With the rising levels of adoption, Security technologies have multiplied too. There is a wider range of options although at the core all represent the same approach to computer-mediated communications (i.e. the growth of indirection, as we analysed in Chapter 3 of this book). The existing technologies offer sufficient capabilities to enable and secure services across a multi-tier architecture. These techniques -Federation, WS-Security, SAML, XACML, SPML, Policy and Attribute-based Access Control, allow us to solve technical requirements and facilitate the introduction of "Cloud Services." Newer, simpler technologies like OpenID increase the choices.⁶

So far, progress for the Security disciplines has been slow in Cloud Computing due to a conceptual confusion. I also pointed to the lack of understanding of the role of the user in the expansion of the Cloud, but there are other issues that compound the problem and limit our role in this new period. It is interesting to see business leaders and teams everywhere promoting Cloud adoption, while IT managers and strategists use the language of Security as a way to slow down this process and retain the technologies “on premises.” This is done under the general assumption the new hosting environments are “less secure” than those run by organisations “in-house.” The industry press is full of talk about security “concerns” with Cloud-based solutions, but professionals are beginning to counter these with very good reasons.⁷

It may be tempting to dismiss these concerns by pointing to the severe security limitations of traditional “Enterprise” environments. In this book I discuss for example the unceasing problem of “data loss” in standard corporate computing environments. It would also make some sense to explain how hosted environments operating around the world have higher levels of traditional security than the usual corporate data centres, but both approaches would be insufficient to explain what is behind negative opinions about Cloud adoptions and assumed Security “risks.”

First we need to understand the problem, and the real challenges to “Security in the Cloud” will become clearer. In my opinion, we have not made more progress in Identity management in the Cloud (which is the essence of access control!) because of the dominance of limited definitions of Identity and Security management. To be more precise I should say the excessive focus on Protection disciplines is making it more difficult to resolve these problems. In the same way as the standard techno-centric thinking obscures the understanding of Information in general, it also affects the debate

about Identity in the Cloud by imposing a limited view of the Security disciplines.

My own approach is to consider four Security Perspectives, each one with its own concept of Identity as follows:

- Identity as value and subject
- Identity as role and membership
- Identity as substance and object
- Identity as context and process

For the Direction perspective, information and identity appear as value, more specifically as subjective value, according to the metaphor of “defining trust” that lies at the bottom of this perspective.

For the Selection perspective, information and identity appear as a role, concretely as membership into a social or organisational group. The metaphor “allocation of trust” is the key to this.

For the Protection perspective, information and identity are understood as an object, as substance. The assumption is that identity can be reduced to data structures “flowing” in the IT machinery. The guiding metaphor is “enforcement of trust.”

Finally, for the Verification perspective, information and identity are relative and depend on the context and the organisational process. The assumption in this case is that identities will be valid or verified depending on the context, under the “verification of trust” metaphor.

How does this help in the debate around "Cloud Computing" and “Identity in the Cloud”? The first result we obtain is to open our minds to different levels and modalities of “identity.” When considered in the whole, in a synthesis of the four perspectives as it were, Identity does not appear anymore as a static object that needs to be stored, hidden and “protected” but as a relationship, as a function, a role, a status, as a moral and subjective value.

At that point the IT mechanisms become less relevant, and the disciplines of Direction, Selection and Detection become more important and decisive: we then discover there cannot be a “technological” and techno-centric solution to the issues raised by Cloud computing (cross-domain authentication, federated identity, identity propagation, data protection and privacy concerns). A unilateral techno-centric solution is impossible because it will necessarily miss the aspects of Trust definition, allocation and verification.

The technologies, mechanisms and software protocols we have offer sufficient ways to negotiate, secure and verify trust, but trust establishment is originated and “happens” outside of the technical realm altogether. It is a compact based on reputation, authenticity, respect, responsiveness, viability and other values. It exists in the social and economic level, outside of the technical sphere of

Protection and Trust enforcement. This reality escapes the techno-centric perspective.

IT disciplines are aware of the need to understand and factor in areas that are outside of the technical sphere. So we speak often of “people, process and technology” as a well-balanced approach. This is not sufficient. If we limit ourselves to analysing factors related to “people, process and technology,” we will be unable to explain what Identity management is about. We may still cover the aspects of “provisioning” people, “controlling access” to systems, and “ensuring compliance,” but we will be unable to address the fundamental issues around data ownership, business models and enterprise architecture. We are missing the whole picture.

If we accept this, we will see that lack of progress in establishing a firm grasp of “Identity in the Cloud” comes from conceiving Identity as an object, or as a physical substance. From that limited perspective, “Identity in the Cloud” becomes a matter of storing, sending, copying, encrypting, marking, enveloping data. By limiting our work to this approach, we use the multiple protocols that have been devised to achieve this (e.g. SAML, SPML, XACML, OpenID) as if these were complete answers to the challenges of Identity in the Cloud. The Cloud has changed the Network, but Security as Protection has not changed and in this sense it has become an obstacle itself by defending the fantasy of a “more secure” Enterprise computing realm.

Contrary to this trend I propose that we base Identity Management Cloud Services on the following guidelines:

- Establishing and governing Identity Data Ownership as the base of the Definition of Trust.
- Developing new protocols for the development of collaborations, partnerships, memberships and roles, as the base of the Establishment of Trust.
- Adopting Policy, Role, Capability and Attribute Authentication and Authorisation solutions as the next step in the Enforcement of Trust.
- Standardising Identity Data, Identity Propagation and Identity Assurance processes as the base for the Verification of Trust.

Identity Federations

If there is any one technology that enables identity management in the Cloud, that is the technology of Federation. This is a small area in Security which is bound to grow in importance with expanding “Cloud Computing.” Originally, federation technologies were proposed as solutions for major organisations, typically surrounded by a number of “service providers.” The idea was the central, large organisation would act as an “identity provider,” vouching for its employees, so these would move freely into the service providers’ applications. The basic “federation pattern” enabled a form of trust between web services, so users authenticated by the “identity provider” would not need to sign into the “service providers.” There were many problems with this approach, and the technology was not successful.

The federation model can have many varieties, but essentially a federated access management solution will respond to the following question: “In the offering and delivery of online products or

services that involve multiple supplier organizations and multiple categories of users, how can these organizations and their clients, members, users, etc. obtain a seamless navigation experience whilst maintaining per-organisation user identification, access control and audit trail?"

These requirements arise in consumer-facing and inter-organisational scenarios, as well as internal Enterprise settings. The term 'multiple supplier organisations' here can imply any operational units that need to maintain some degree of autonomy - it can mean legal entities, companies, divisions, geographical business units, governments or departments. So the key terms are as follows: "online products and services," "multiple supplier organizations and multiple categories of users," "seamless navigation for end-users," and "per-organisation identification, access control and audit trail."

These four conditions essentially say the value of any federated solution lies in the fact that a supplier organisation -- a "service provider"-- will benefit from the reception of traffic from end-users who are not registered in their user repository and do not need to authenticate with them. In reality though, the "service providers" always had to have some form of user data store, even if they did not authenticate the incoming network traffic. For example, a health services provider for a major organisation obviously had to have relevant identity records for the end-user. In practice, users were managed in multiple sites anyway despite of so-called "federation arrangements" and "circles of trust."

In a transformed global network, federation technologies are having a different role. While in the past these technologies responded to the need to have some form of simplified sign-on or cross-organisational authentication, scenarios where one major organisation acts as the single or main "identity provider" are rapidly becoming a thing of the past. We now see "networks of networks" and the expansion of a wide array of partnerships between organisations. The new network does not have a centre and the actors are peers in their informational exchanges. Instead of focusing on a "shared" repository of user identities -- owned by the "main participant"-- we see instead many partners in the Cloud, each managing users separately but still collaborating at many levels and trusting each other.

Initial forms of federated access were implemented with ad-hoc mechanisms and customised credentials carried in the Internet protocols; later on, the Security Mark-up Language (SAML)⁸ brought much-needed standardisation and transparency to these solutions. In this new and more complex scenario, organisations are beginning to realise that a federation solution effectively liberates them from the need to manage all the users in a single place, but to fully exploit this realisation, a conceptual change is needed.

My point here is that the best scenario for federation architectures, where these technologies will flourish, is one where user repositories are not "shared" across organisations, and where there is no need to manage the users centrally to provide them with the much-sought-after "seamless navigation" from one service to the other. In the Cloud, which is a "limit case" of the evolution of federation technologies, the original pattern of access cancels itself as the maximum benefits can be obtained when user management requirements are small. This is the context where Security experts need to start thinking of even more advanced solutions where trust management is not articulated around an

ideology of “attack and defence” and “protection,” but around a complete vision of enablement and inter-organisational trust.

Cloud Security Concerns and Advantages

When Security experts and practitioners gather to speak about the Cloud, generally their concerns are one or more of the following:

- a) Data security. These are perhaps the most frequent concerns, rooted in the perception that Cloud solutions somehow expose data more than “corporate” computing. This concern is understandable, but the discussion needs to evolve; for example, recognising the same safeguards that exist in corporate computing are equally possible and necessary in the Cloud. Instead of assuming that Cloud environments are intrinsically less secure, we should understand why Cloud providers have been working on a “best effort” basis and have not offered comprehensive solutions for data encryption, user separation (segregation), and high assurance levels. In the end, the market cycles will bring these higher-value services to the foreground and data security concerns will be resolved. Current “software as a service” offerings frequently lack enough Security safeguards regarding direct access to data stores, segregation of duties, cryptography and client data isolation but that can also be resolved and is not different from current corporate environments.
- b) Data Privacy. Regarding this area there seems to be a fundamental contradiction between Cloud providers and the legal obligations of their tenants or clients. There is for example a very relevant interest from organisations to avoid cross-border data transfers, as well as transfers of liability to third parties. While it is clear that accountability cannot be transferred, Cloud providers have so far given an uneven response to these concerns. It is necessary to work out better arrangements so the Cloud services can perform as “data processors” (not as data owners), but can be bound by appropriate contracts and legal safeguards to increase the confidence of the consumers. The following areas need to be covered in data processing arrangements: data provenance and transfer, data linking or aggregation, data lifecycle, legal obligations, limits of data collection and use, data retention and audit trail duties, data destruction policies, data-centre certification and regulatory compliance. A point of interest here is that the industry is paying a lot of attention to business and government concerns about these issues, but less so to the individual citizen’s concerns (which I will cover in a later section of this chapter).

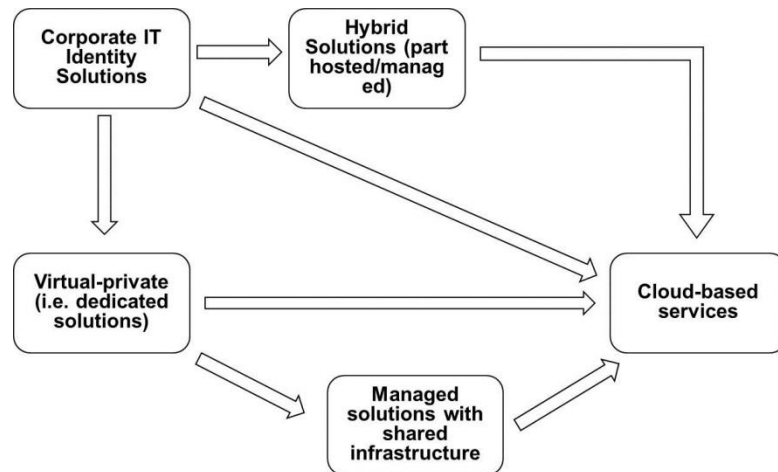
The concerns listed here have to be recognised and addressed. At the same time it is important to remind the Security disciplines of the essential advantages that Cloud computing brings to all types of organisations, and we also have a role there. If the Security disciplines do not understand our contribution to risk and trust management in the whole and remain anchored in the “protection” era, we will be unable to see how and why the Cloud is changing the private and public computing landscape for good.

Above all, without letting ourselves become distracted with marketing messages and “new” technologies that are not new, we need to acknowledge Cloud computing fundamentally changes the

cost and benefit relations for all types of organisations and businesses. As more and more services come into the Cloud, providers and consumers adopt a utility cost model. This change is happening despite the resistance of major software vendors attached to traditional multi-year “maintenance” contracts and software fee renewal payments. In the case of Identity management, the new model translates as a cost per user (per month or per year). In the recent past these flexible commercial arrangements were known as “subscription” contracts, but that terminology still was linked to the prevalence of software licencing. In the more recent period and in the future, software licences and “maintenance contracts” will recede into the background, as the consumers will want to pay exactly for the service they receive (at a market price) and not for the “privilege” of using a particular brand of software or hardware.

Cloud computing in fact represents the increasing power of the consumer, the market, upon industries that operated for too long in a vendor-driven environment or “push” market. For sure, the transition is not complete, but the industry will get to the long-predicted “utility model” in computing.⁹

The second focal point in assessing the Cloud has to do with the fact there is no single class or type of service. Marketing campaigns do a lot of harm when the term “Cloud” is used indistinctly for many forms of this economic and business trend. Doubts regarding the quality and the security of these services are increased if the consumers believe there is a one-size-fits-all technology. In fact, many types of Cloud solutions will coexist for a long time and Cloud adoption will have many routes.¹⁰



Organisations may move directly or indirectly to Cloud solutions

A change in the pricing model means a change in the cost structure of the consuming organisation. This is very positive, but we also need to take into account benefits arising from and the elimination of overheads and project costs that are implicit in corporate computing. What organisations do now in one to three years in Identity management, they will be able to do in one to three months!¹¹

Information Technology and Capitalism

What we are seeing then is not the appearance of new technologies but the result of the global actions of users and organisations, expanding the use of computing platforms and following a very normal path towards cost reduction and profit maximization. This is how the Cloud operates and what the Cloud is. It is a social and economic phenomenon that deserves understanding and action at the same level. In other words, it needs a social and economic conscious action instead of a techno-centric approach.

Identity management will not progress if we do not grasp that Information technologies are the fruit of late capitalism, and the Cloud is the latest evolution in this space of action. Computers in the global network dissolve the personal mark of any activity, through indirection and anonymity. When computers were first implemented in organisations, we also saw resistance to their adoption, similar to what we are experiencing now in relation to the Cloud. The deeper reason for this was that computers facilitated the abstraction and indirection of human activity, thereby transforming many organizational processes and directly affecting the workers and managers. The traditional corporate worker was effectively replaced by a new class of specialists and managers.¹²

Another cycle of indirection is afoot now, whereby corporate computing will gradually disappear as we know it. It is normal and natural that many people resist this change, but it will take place anyway, in the same way as in a preceding period the business computer transformed economic and social activities. The personal computer materialised the generic, interchangeable nature of work in the global network, and there is no economic reason or way to stop this movement.

While the essence of computation predates capitalism by thousands of years, capitalism re-creates the computer as a generalised tool for generalised activities. The personal computer is of the same order of reality as the car and the telephone. Like these, the computer is not only an “extension” of the body, but also a generalisation and automation of human activity. While it is usual to speak of the computer as a brain-like entity, it is much better to consider it as the automation of manual and visual activities: reading and writing. In fact, on close analysis, everything the computer does for us (or with us) is to read and to write, as I commented in a previous Chapter of this book. Not only does the computer take over the space of the typewriter and the book, but the space of the hands and the eyes altogether.

So the computer needs, reinforces, educates, introduces and enables generic action. The generic worker creates the computer and is created by it at the same time. The technology, so to say, breeds its consumer, the individual characterised by post-cultural, post-national, multi-faceted activity. In the space co-defined by the generic worker and the generic tool (the computer), Identity is characterised by a context of more indirection and more fragmentation, and this has very important consequences for the Security professions. Let us now consider how these effects appear in public (citizen) Identity management.

Identity Assurance Services

The essence of the “assurance market” proposals is to engage the private sector to develop identity assurance services for public and commercial electronic or digital exchanges. Such assurance services would ensure that citizens and customers could easily and securely provide trustworthy identity and other personal information to the Service Providers.

This stance represents a new direction in the thinking of the public agencies and technology organisations in and outside of the Governments. In the past, the consensus position was to aim at centralised authentication services in the form of Government Gateways, or “bridges,” supported by publicly-managed assurance mechanisms (using official identity credentials). For example, the Belgian and UK public gateways were designed to operate as a generic federation hub for all government departments.

The new stance shifts the provision of “assurance services” to the private sector. During the debate, the proponents of this change suggested generic benefits of extending digital services to a wider part of the population, more or less the same benefits as those advertised in previous centralised “gateway” strategies.

The change to the new schema is justified in terms of reducing the complexity and number of the user authentication mechanisms required by public entities within a general move towards e-Government. Payment and benefits fraud is also a consideration, but not in all cases, as the main driver seems to be reducing operational and authentication-related costs for public services.

The main positive factor in favour of the new approach seems to be that the private sector would help the government to accelerate digital services adoption, but it is not clear how. Countries with different levels of national identity policies and instruments also have various approaches to this problem.

It is not clear, for example, how multiplying assurance services would facilitate e-services adoption. In fact, even in strong commercial, legislative and regulatory environments, it is not clear how a diversity of assurance services would help with wider or faster adoption. Obviously where that regulatory and market environment is missing, the problem is even deeper.

I think there is a lack of understanding of the effects of multiplying “assurance services” and some level of confusion between the different concerns of “identification,” “assurance,” “authentication,” and “identity provisioning.”

It is clear the e-services strategy held by various European governments is based on the goal of reducing the cost of identity assurance by creating an “assurance” market, hopefully with the concurrency of the private sector. There is an expectation that a Government-created market (which would be supported by making it mandatory for citizen-agency interaction and transactions), would be able to reduce the cost of “assurance” for the government. This motivation should be at the centre of the discussion, instead of the more generic suggestions the strategy would primarily “improve” services for the citizenry.

The assumption that private assurance services would be commercially priced but mandatory -- while at the same time being diverse -- does not seem to reflect appropriately either on the costs for the citizens nor the business case for the private sector. If the cost-reduction driver were clearer, the discussion would be more productive.

The key problem hampering this vision is that intended commercial, legislative and regulatory activities are focused on users of public services. What about the private service offerings? In theory, the same private assurance providers could also sell services for other markets, but it is unclear how a Government-mandated and regulated sphere of services would coexist with the unregulated services. This uncertainty would need to be removed, perhaps with a different approach, to gain more private participation.

The proponents of these strategies also assume that a significant segment of society in each country will not use digital public services, or may require personal assistance when using these. The strategy would not work then if the market did not develop appropriate offline services? Here we see a potential conflict between the drive to reduce operational costs, the transfer of assurance services to the market (effectively the citizen-consumer) and the potential denial of benefits for the entire population.

At a different level, in terms of Security Management concepts and principles, the assurance service strategies pose important challenges for the private sector experts and leadership: While the main direction of the strategy is to form a “market” for “assurance” services, there is a non-explicit assumption there will be a market for “authentication” services. In other words, there is confusion or at least a conflation of two different security capabilities (authentication and assurance).

The term “assurance” should be used in the context of user identification and verification (ID&V) and should be treated separately from authentication capabilities (i.e. online credential validation and authenticated user data propagation). The term “assurance” is frequently used incorrectly, conflating the Identification and Verification process (ID&V) with the Authentication process. It is true that almost all services—public and private-- require the user to go through some form of initial registration and then through subsequent login procedures. These two steps have different requirements and practical solutions, but in many public and industry documents we see they are not differentiated.

The question arises about the proposed “assurance” services: are these focused on the ID&V phase or the authentication phase? Will there be a combination of the two? This differentiation will become critical in time, because if an “assurance services” market is created and made obligatory – independently of what we may think about the notion of a compulsory “market”-- not all participants will have the same ability or interest in “assuring” as well as “authenticating” an identity.

Greater levels of assurance come from the combination of multiple identity instruments or credentials, especially those which can be traced back materially (physically, biographically, biometrically) to the biological individual. What is then the exact meaning of assurance in this context?

The lack of differentiation between “assurance” and “authentication” generates other complex problems which need to be addressed. A private “assurance” provider with access to public information (for example birth records or passports) will have more “assurance quality” than a provider selling “assurance” on the basis of privately-operated ID&V or with less capacity to aggregate such data. On the other hand, an “authentication provider” does not need to be an “assurance provider,” but just operate in a federation or “circle of trust” with the “assurance” provider. Once this is understood, it will become clear the “assurance provider” may or may not be in possession of original identity data. In fact, in more technical terms, the current “assurance market” initiatives have weak distinctions between four interrelated but never identical Security concepts: “Identity Provider,” “Assurance Provider,” “Attribute Provider,” and “Authentication Provider.”

In the standard Federation architecture the Identity Provider is at the same time an “assurance,” “attribute,” and “authentication” provider, given the fact the main participant in the federation is also the “owner” of user ID&V process and data. Differently, in more advanced scenarios the four functions indicated above are separated. For example, an “assurance provider” could operate with identity data provided by a government agency, while the authentication provider could be a trusted third party in a federation.

If we consider a functional differentiation of the processes, questions arise about ownership of the data, data privacy and data protection. I believe that none of these questions has been resolved either in the public or the private sector in the context of the “assurance market” initiatives.

It is important to see that if the level of “assurance” provided by a private organisation depends on the quality of data provided by public agencies, it is difficult to see how this will match a strict public service rationale for the proposed scheme. Another conflict becomes clear: between cost offloading to the market (the consumer) achieved by means of commercialisation of citizen and consumer data.

This takes us back to the initial centralised e-government strategies. Originally, these directly sought to use the identity data stores in possession of public agencies in order to build standard “federations”; now, the assurance market proposals assume that identity data stores of the consumers will be a highly diverse mix of data repositories under private and public ownership, as well as private aggregations of citizen identity data. This contradicts the general goal of government-validated identity or central authoritative sources, while it relies on exporting the assurance function to the private sector. The situation will be quite different depending on the type of data the public agencies are able to master and provide.

In some countries, private providers –if they find interest in this market–will need to use national identity cards to reach a high level of “assurance”; while in other countries public information will be more diverse in quality and coverage (for example entire segments of the population may be missing from certain types of sources).

Therefore, in the whole, the consequence could be not only that operational assurance costs are off-loaded to the public, but also that assurance quality could become uneven and would not have a direct

link with public authoritative sources. The loss of a direct link may be moderated by means of regulation and industry standardisation, but this opens a wider discussion as to the use of data, data privacy, end-user opt-out rights, data ownership, and data access rights.

Another implicit inefficiency of the proposed strategies is the generation of different (probably many) identity data stores both in and out of government agencies with differing quality, integrity, completeness, etc. This means the overall costs (at the national level) of identity verification would be multiplied. Nothing would ensure the convergence of the identity data stores even if the Regulator controlled the new “market,” because the private suppliers would aim at the lowest cost of providing “assurance” for the mandatory transactions. On the other hand, premium services, which already exist for other markets, will rely on different, higher data quality and more complex data aggregation processes, hence increasing and not lowering the heterogeneity and overall cost of the identity data stores.

It is frequently assumed that a citizen-customer will not have to register with each digital service, and that he or she will not have to remember login details for each one. This is another level of the problem, and a consequence of the conflation of assurance and authentication. The problem is the “assurance market” proposals wrongly expect that it would immediately ensure a uniform use of “authentication” credentials across services. The implicit assumption is the authentication technology for the entire market would trust identities validated by the “assurance suppliers.”

This is normal in Federated Identity Management architecture, but in those cases all the participants in the trust circle have interoperable technologies and standards and also direct or indirect (transitive) trust relationships between them. It is evident the strategy proponents expect that all providers and all participants in the scheme will have to invest and update their security infrastructures.

Precisely because the schema would require investment and infrastructure updates, coexisting assurance providers, identity providers, attribute providers and authentication providers would increase the need for the public agencies to validate, maintain and secure citizen data and their own security solution’s infrastructures. For example, for each public agency it will be necessary to implement an identity data, attribute mapping service to correlate trusted identities with the local data stores.

It is therefore not advisable to think that it will be easy for the public services to migrate all their users to the new schema. In fact it should be expected that most public agencies will need to continue managing their users and will want to do so.

In the medium to long term several approaches to the assurance market will coexist, based on the distinction between assurance and authentication, and developing new federation architectures with separate roles for identity, service, attribute and assurance providers. In all cases though, we will also see distributed Identity data management, and hopefully also an increasing adoption of user-centric assurance and authentication solutions.

Identity Trends

As a conclusion for this chapter, I would like to list several trends which sum up the current transformation:

- The protection and compliance focus which Identity management inherits from the Security Domain will not disappear, but it will have a lesser role in the IT landscape than it has now.
- Centralised control models over identities will be reserved for restricted areas of the IT infrastructures, while at the same time organisations implement federated and decentralised assurance services.
- Privacy and Data Protection concerns will be seen as essential, but increasingly not as a central management task, and instead as rooted on the individual choices and different varieties of identity.
- Identity management as a Service will experience rapid adoption but a single model will not exist, and corporations will sometimes have partly hosted and partly on-premises solutions.
- The intellectual structure of Security and Identity management will change, moving from a focus on Risk Management, to a balance of Risk and Trust Management.
- Given the perceived and real risks of network crime and disruption, security will rely even more on defences in depth, and a variety of identities and identity assurance levels while deploying more refined risk-based and attribute-based access controls (all of this enabled by Identity management solutions).

With Cloud Computing, we will see two major trends arising: Security and Identity “for” the Cloud, and Security and Identity “in” the Cloud. The first represents Security mechanisms and services to protect the Cloud (i.e. hosted, shared) environments; and the second represents Security products and services offered by managed, hosted Cloud platforms. The two are inseparable and will coexist for a long time, while simultaneously we will see a constant reduction of the role of corporate computing.¹³

¹ IDC research indicates worldwide investment in cloud computing will treble between 2010 and 2013 when it will reach an estimated \$44.2 billion. IDC Cloud Research, http://www.idc.com/prodserv/idc_cloud.jsp

² “Worldwide revenue from public IT cloud services exceeded \$16 billion in 2009 and is forecast to reach \$55.5 billion in 2014, representing a compound annual growth rate (CAGR) of 27.4%, a newly published International Data Corporation (IDC) document finds. This rapid growth rate is over five times the projected rate of growth for traditional IT products (5%). This research further illustrates that public IT cloud services are crossing the chasm with modest revenue, but very fast growth.” The IDC report was cited by BusinessWire.com: <http://www.businesswire.com/news/home/20100623005419/en/2014-Public-Cloud-Services-Grow-Times-Rate>, 2010

³ Source: <http://www.ibm.com/developerworks/webservices/library/ws-soa-simm/> IBM Service Integration Maturity Model (SIMM), October 2005

⁴ The direction set by the Forum is synthesised in the “Jericho Forum Commandments,” version 1.2, May 2007. This document clearly addressed the “deperimetrised” organisations of the present and future. This is already a reality in transnational corporations. The “fundamentals” section of the document in reference describes three areas which can be aligned with my own Security model as follows: 1) “The scope and level of protection” can be aligned with the “Direction” perspective, but two elements of the detail, “basic protection” --individual systems capable of “protecting themselves”--- and “closer protection” for assets, can be aligned with “Protection” perspective for additional clarity. 2) The “Security mechanisms,” including the details, can be aligned completely with the “Selection” perspective. 3) The “Context” can be aligned with the “Verification” perspective. This is a very fine and forward looking document that should be obligatory reading for Security architects. It could be improved by a more precise combination of capabilities so that the reader can determine in practice when an organisation has transitioned to a deperimetrised context.

⁵ Together with Cloud adoption, organisations experience an internal maturation process which ideally will end with the creation of Service Inventory Endpoints, i.e. well-documented service interfaces for legacy or web applications. Among these, Authentication and Authorisation Service Endpoints are also possible and desirable as these can immediately become the basis for Identity Federation services. This evolution is now visible in a small number of global organisations but

its generalisation is not guaranteed. For a detailed explanation of the SOA Service Inventory Pattern see: SOA Design Patterns, Thomas Erl, Prentice Hall, 2009 ; and <http://www.soapatterns.org/>

⁶ The best place to start to learn these standards and projects is the Oasis web site: <https://www.oasis-open.org/>

⁷ See for example this article by Mike Fratto in Network Computing: <http://www.networkcomputing.com/public-cloud-tech-center/public-cloud-is-neither-more-nor-less-se/240002750#>

⁸ SAML version 2.0 is an OASIS Standard: <https://www.oasis-open.org/standards>

⁹ IBM has been “predicting” a world based on “utility computing” for many years, a long time before the Cloud trend started. See: <http://researchweb.watson.ibm.com/journal/sj43-1.html>

¹⁰ The diagram shows several possible “routes” for Cloud adoption for large organisations.

¹¹ This comes directly from my experience in major projects in Europe where I have observed excessive costs in standard corporate programmes (higher than Cloud computing by a factor of 10).

¹² Consider for example the impact of Information Technology on business downsizing and restructuring in the 1990s. See also: Grant W. Lawless, “Information Technology (IT) For Manufacturing: Where Has It Been, Where Is It Heading?” Journal of Industrial Technology, 2000.

¹³ See: Nicholas Carr, “Does IT Matter?”, Harvard University Press, 2004

7. Quantitative Identity Management

Information value and flow

As Identity becomes data with the global changes in Information Technology and organisational transformation, so the emphasis moves from Identity as a security item, to performing Identity data exchanges. It is a commonly accepted notion that information "flows" from one point to another, from the emitter to the receptor, inside and outside the organisation. This is a one-sided view associated with one of the four possible Perspectives or metaphors that I use in this book: the Machine metaphor. Within this perspective, Information is seen as a substance that flows from point to another. This opinion is associated with the belief that information flows in one direction, and that it is possible to speak of information as a one-directional flow of "data." Other chapters in this book cover the implications of this view, and how it affects the practice of IT and Security management.

I think the mechanistic definition of information has a place in organisational and business management, but taken in isolation, it has counterproductive effects and leads to a wrong understanding of the challenges of Identity and Security management. The essential problem is that mechanistic definitions ignore that any signals arriving at the Receiver need (even in an electro-mechanical model) some form of enablement, activation or detection, so the signals are perceived at all. Interpretation of the signals also needs a complement of filtering, comparison, synchronisation and other Receptor-side capabilities to "make sense" for the party acting as consumer of the information.

The techno-centric view takes for granted that the receptor is already enabled in such a way that a unilateral flow of information from the "emitter" will "make sense," but that is just an assumption and not an understanding of what is happening. What activates and enables the receptor? For any information perceived by the receptor there must be at least an equipotential information (a structured signal) emerging from the receptor itself. More generally, the receptor must be tuned to the signal. A good image of what happens at a physical level in a communication channel is that a "computation" takes place by which two tuned and correlated signals enact a two-way exchange between the emitter and the receiver.

At a different level, when we consider not only the technical or physical layer but also the organisation as a whole, the same principles are valid. The best approach to information exchanges is one where we assume not a unilateral flow but at least a two-way exchange of data. Translated to the business view, a good explanation must make use of the idea of the "value chain." This approach refuses to attach value to information itself, and instead judges the benefit of a process by the results of the production and distribution processes as a whole. The information exchange is a facet of the business process and is multilateral in nature. In this scenario, information and data become mediations and signals of the value process.

This leads us to an indirect way of measuring the value of information, one that does not need to think of information in terms of an object or “thing” that can be stored. In fact, in this approach, information is simultaneously a thing (a mark stored in electronic media) and a relationship (because stored data only becomes “information” when it is exchanged, and when it is subject to read and write processes by the participants).

In other words, information has no value until it arrives at the consumer, and this can be either on the emitter or on the receiver side. As there are consumers on both ends of the information transaction, we should also consider a new terminology and stop talking about an origin and a destination of the flow of information. Both ends are simultaneously “emitting” and “receiving” data.

Continuing with the image presented in chapter two, if a “secure,” “protected” environment has no information exchanges with the “exterior,” we could say that what needs to be protected in a Security strategy is not “information,” but the combined techno-economic or socio-technical process that provides information to the consumers (on both ends of the transaction). More generally, we could say these consumers are of various types, not only business management decision-makers but also all other types of individuals involved, including the consumers and operators in the production and distribution process.

Losing the ideology that we should work to protect a “thing” or an object will help us to address the challenges and solutions required for a business value chain and its information processes. In “The Management Information Value Chain,” Robert L. Phillips proposes an indirect way of measuring the “value of information.”¹ Focusing in particular on “management information,” Phillips writes: “A management information system helps an organisation make better decisions. [...] Perhaps the most common barrier to achieving the goal of competitive advantage is that management finds it difficult or impossible to measure how management information systems contribute to corporate value. Without this understanding, it is difficult or impossible to evaluate investments in management information systems on a basis consistent with other investments. As a result, management information system investment decisions are often based on arcane technical considerations that only specialists understand, and escalating MIS costs do not seem to be matched by corresponding benefits. No wonder many companies have found obtaining competitive advantage from their systems to be elusive.” To correct this, Phillips suggests the utility of management information systems and supporting activities is to provide information that enables better decisions. In this sense, the value of management information is equal to the increased profitability resulting from the better decisions that it enables.²

The idea is simple and can be generalised beyond the “value chain” method. Most importantly, by assuming a bi-directional or multidirectional information exchange process, we will see “decision-makers” not only on the side of “management.” Every information producer and consumer is a decision-maker. Therefore, the value of the information processes and the systems supporting these can be measured by how they perform in enabling those decisions. If we consider how Security and

Identity solutions enable information exchanges in an organisation, we will immediately see that confidentiality, availability, integrity and quality of information are required on all ends of the information network and the results of any investment in this sphere can be measured by how the solution supports decision-making. It is important to see that Phillips does not attribute an intrinsic value to information, but assigns all relevance to the process of "converting data into information," i.e. into a business process.

If the conventional perspective (centred on Protection of assets) prioritises the "flows of data," the new perspective—with a complete integration of the objective and subjective views—must underline the flows of identity data. We can still accept the relevance of data movements (even under the fictitious image of a material flow), but this has to be complemented with the correlated identity flows that interact with the data flows. If data transfers are the weft of the network, identity flows are the warp. One supports the other so the "value of data" materialises when users are enabled to consume it in many forms, and the "value of identity data" is realised when it is applied to business data transfers.

This becomes more visible if we consider the "extended enterprise business model," meaning the data and identity exchanges across the value chain or value network. On the technical side, it has been observed that higher performance requires a tighter integration of the Information Technology systems across the extended enterprise. External users require access to systems hosted by the organisation and internal users need access to systems hosted by partners and service providers. Equally important are those requirements where organisational and external users need access to Cloud-based services that are outside both of the enterprise and the partner authentication domains. A mobile, diverse and geographically scattered workforce becomes more and more the reality of national and global corporations and especially of the new "virtual" organisations.

In this context, the "value" of information is dependent on the interplay of identity and business data, and the key questions are no longer those of "Protection" but those of "Selection" (Trust Allocation and user enablement).

Identity and Organisational Transformation

Many times, I have been asked, "What is Identity management and how does it work?" Many Security professionals are still unsure about the scope and nature of this discipline. Identity management is above everything else a Security discipline where the ultimate goal is to achieve efficiency and organisational excellence. It was already relevant in all types of organisations where informational processes are more or less well "protected," but Identity data is not considered an asset and is not managed with appropriate processes. It is more relevant in a stage where the majority of users are not within the organisational boundaries. It would be an error though to see Identity management as just a way of reducing complexity and costs of user management. We can do that for sure, by means of automation and workflow engines, but would reduce Identity Management to a normal technology-centric discipline. The truth is that neither automation nor workflows nor the desired user

management tools can work by themselves, and Identity management always has a very strong component of organisational transformation.

Within the conventional framework, Identity management tended to put much emphasis on setting up role-based access controls. This still makes sense today for some areas of the organisation and some sets of applications that require an approach based on roles, but in the expanded enterprise, it is difficult if not impossible to express Identity management requirements in terms of an organisation-wide role model. Neither the diversity of applications, nor the variety of users and locations allow for a single model, and hence it is essential to have a more flexible, distributed approach. It is necessary to consider other ways to "manage" external identities, for example self-service, third-party registration, lightweight authentication and federation services. The "roles" of the external identity types cannot be defined in the same terms as the "internal roles," as these depend on data owned by the organisation under employment contracts and job definitions. On the other hand, this evolution is leading to the recognition that external users should and can only be managed by the external entities themselves (including the assurance providers and the individuals involved).

Corresponding to this, the main direction of the effort is now not towards access control, but to access enablement. Selective enablement, providing access to a deeper, more complex and layered set of assurance levels finally amounts to access control. The emphasis is on giving access and selectively enabling access channels, so the control objective is achieved in a different way.

This different approach also means the focus is now on performance of the entire identity and data exchanges, and not on security. In the past, Identity data was primarily bound to separate "silos" or islands of IT solutions, and the evolution of Identity management was dependent on the upgrade and improvement road map of the other areas in the IT departments. In the new period, Identity management becomes less technological, more standardised, and moves both inside and outside of the organisation. In this sense, it becomes more and more independent of specific platforms or technology brands.

Today it is still difficult to see the result of this evolution, but the first steps have already been taken by many organisations, especially those that have seen the complete failure of attempts to centralise Identity management following the "enterprise" model. The current emphasis on regulatory compliance, driven by legislation, also obscures the underlying transformation but will soon leave the forefront of business concerns, as people begin to see there are audit issues precisely when Identity is not owned and managed, whereas the Compliance emphasis is currently 100% reactive and improvised, and thus repetitive, costly, expeditious, and unsustainable.³

In the new period, too, when Identity becomes data, the focus is on performance. By this, I mean the performance of the information exchange network as a whole. When speaking of performance, what I mean is Quantitative Identity Management, as announced by the title of the present chapter, but we still need to cover some other points before addressing the new idea.

What IT never did, and never will

When reading the current debate about the future of IT and Identity management, we see how a large part of the Security expert community is still trying to "save IT by means of IT." It would be suitable to analyse all the motivations for this stance, and see for example why the IT professions are so attached to the survival of the traditional IT department in their organisations. Nevertheless, such analysis would go beyond the subject of this book and must be left for another time. Here I want to look only into the context in which Identity management is becoming a quantitative discipline even if the majority of the experts cannot recognise this.

Professionals react to predictions about the Cloud with either disbelief or smiling contempt. It is visible that IT professionals —especially veterans and Security experts—are not comfortable with the implications of the Internet and Cloud computing. Many opinions have been expressed, for example, against predictions the IT Department was becoming a thing of the past and intense debates have been generated by the suggestion that IT as we know it is about to disappear.

So for example, when in May 2003, Nicholas Carr predicted the end of Corporate Computing, his writings were heavily criticised by experts touting the "importance" of IT and the ability of IT departments to "bring value" to the organisations. Carr wrote: "Something happened in the first years of the 20th century that would have seemed unthinkable just a few decades earlier: Manufacturers began to shut down and take apart their waterwheels, steam engines and electric generators. They no longer had to run their own dynamos; they could simply buy the electricity they needed, as they required it, from new utility suppliers. Power generation was being transformed from a corporate function into a utility. Now, almost exactly a century later, history is repeating itself. Information technology is undergoing the same transformation."⁴

I am a witness of this transformation and have seen the evolution of the IT world since the time when the only computers in existence were housed in special rooms and attended by people in white coats. While I have seen the constant change of IT Departments (including in the area of Identity management), I also know IT never did Identity management well. In my mind, the only question is if the IT shops will ever do it well, now that the global transition to cloud-based services does not leave much time for more experiments and failures.

Perhaps the defenders of the IT Department have a point, because since Carr and others started to describe the challenges faced by the traditional approach, the IT Departments of this world have put up a strong fight. Guided by technology vendors with an interest in the existing enterprise platforms, the IT Departments have projected medium and long-term "adoption" of cloud technologies but always in a hybrid modality, as extensions of the current IT roadmaps.

This is reflected in the way technology choices are made. There is a simple way to discriminate which technologies in the market point to the future, and which ones cultivate the past and thrive from the

continued entanglement of IT "solutions." While there are criteria to discover the fit of a particular technology into an IT roadmap, we need to abandon the obvious approach. What does it mean, after all, to "fit" into an existing IT roadmap? In most cases, an IT roadmap will be a succession of upgrades and patches to pre-existing technologies, chosen under different circumstances and under now-forgotten reasons. In this context, "fitting" cannot be more than trudging a path along an already unsuccessful IT story.

For example, in the traditional Identity management, typical services do not extend to user types outside the enterprise boundary. As business expands, it is difficult to share information safely. Federation technologies should address this, but require costly changes for all parties. Small players never adopted Federation, and Partners did not agree who was the Identity Provider, and who would have control of user information. In this context, the Identity management becomes a succession of "upgrades" and "workarounds" where business programmes and both external and internal users have underperforming identity services.

Typical characteristics of the situation are:

- For every I&AM project delivered, there are always two or three in each organisation with severe challenges.
- The "enterprise IT" approach appears unable to address Global requirements.
- Typical challenges include: High CapEx and OpEx.
- Large amount of integration and customisation needed to support business applications.
- Complex, costly compliance management.
- "Solutions" are rigid and expensive to change.
- Technologies to cover employee, partner and joint venture authentication and provisioning with the different security levels and services are difficult to find.

On the other hand, change never stops, propelled by social and economic transformations. As the organisational boundary disappears and business develops based on extended collaboration circles, Identity becomes data and its management moves out of the enterprise for external access routes including mobile workers and consumers. In a short time, Identity services will scale to hundreds of millions of users covering every major industrial and post-industrial economy.

It is a known fact that IT Departments never did Identity management well, precisely because it was involved in a never-ending upgrade path to existing infrastructures and point solutions. As things evolve and the centre of gravity of Identity moves outside of the organisation, will the IT Department still have a chance to "manage" it? Is there room for some new experiment that will finally allow the IT department to do what it always held as a pending task? My take on this matter is that there is no more "time." Even more, I believe the meaning of the historic transformation is that, as Identity becomes data, and Identity management becomes focused on quantitative measures and performance, the complexity and fragmentation of the current IT environments automatically disable these to compete with the new efficiency-focused cloud-based services. There will be more resistance

So, to return to our question: how can we discriminate those technologies that thrive from the past from those that open the gates to the future? The criterion is: look out for those technologies that are there to be “implemented” by IT, or to “help” IT deliver Identity services. These reveal the defensive actions of the IT Departments, which are still trying to remain relevant and hold on to their "realm." Too little too late, I say. These are, in my view, the technologies and solutions that stand in the way of the great transformation.

Within the Enterprise framework, Identity management solutions consist of four layers of technology and processes. These organise the identity data flows and the user access to data with the aim of controlling access and achieving the goals of the organisation. The three layers are:

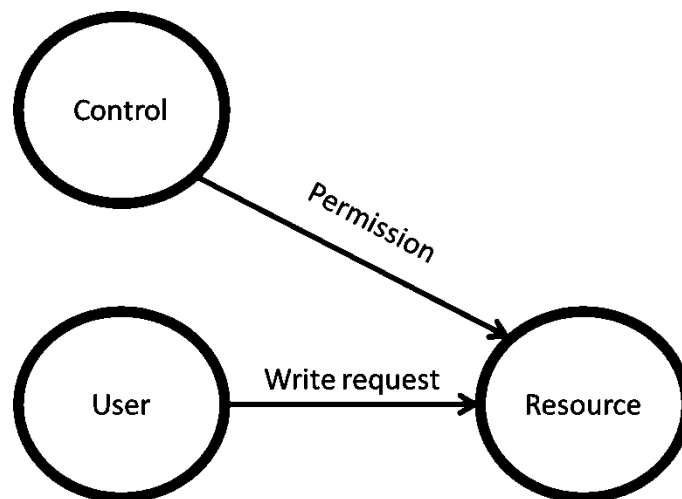
- The following diagram shows the four layers and the various sub-processes they contain.



The Identity management functional layers are interdependent in one direction: the upper layers are dependent on the lower ones. The foundational layer, labelled "Identity Data Governance," is the basis for the full development of Identity management in the organisation. It is useful to see these layers not as a one-off project, but as permanent processes that must be part of business operations.

Starting from this conception, an Identity management programme should have a series of steps or staggered projects by which each layer is built out and uses the resources made available by the underlying levels. Subsets of these capabilities can be implemented in advance of the full maturity of the basic layers (for example before completing the Identity Data Governance capabilities), but in that case those early developments could become isolated, point solutions unable to deliver their full value.

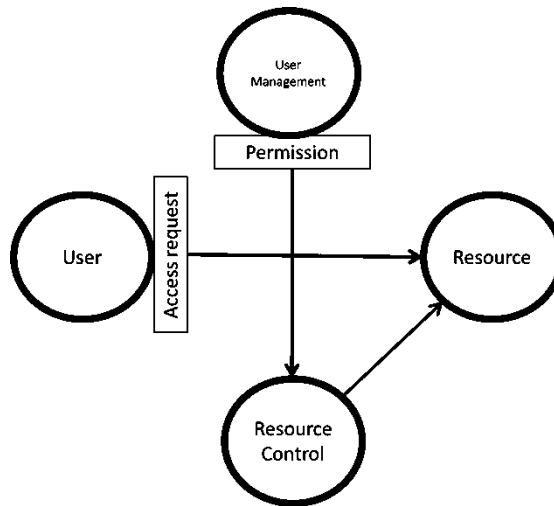
For the purposes of this book, it is important to explain the reason behind this layering of the Identity management solutions. The key to this architecture is the focus on identity as data but in the context of the interactions of users and resources. When considering the simplest case of user access control, we see at least two sets of data in interaction. On the one hand, we have the user access request (to a resource); on the other we have the user access approval. A simple image will reflect this basic fact:



Simple access control interaction (example)

The example is "simple" because the response from the Resource to the User is absent, as well as the interaction between the User and the Control function. In fact, each of the write operations (depicted as red arrows in the diagram) is a combination of reading and writing operations, and is strictly speaking bi-directional in nature.

To picture this we can have a look at another, more complete diagram:



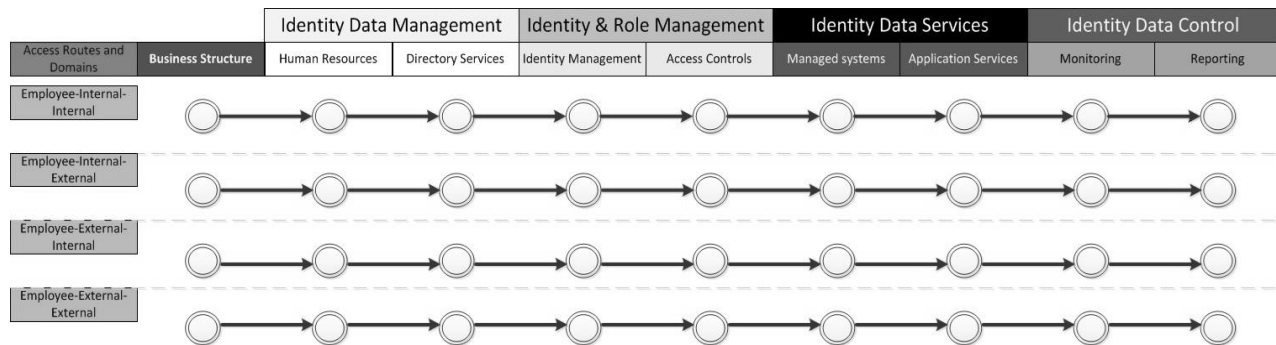
Expanded user access interaction

In this case, we see two "write" operations, one between the user and the Resource, and one between the user management function and the item labelled as "Resource Control." In turn, the Resource "reads" the permission from the Resource Control item. The important point here is not the diagram itself but the interaction of various operations. A more complex and realistic diagram would show the user request going first to the user management function, for example, but in the end all interactions amount to exchanges of information that eventually allow the user to read and/or write from/to the resource.

Fundamentally, however we complicate and expand this diagram, perhaps introducing more users and more resources, or even more steps in the authorisation and read/write operations, we can see there are information interactions that enable other information operations. More specifically, the user management and permission data exchange makes the user access (read/write) exchange possible. For this reason, I put the permission arrow as "crossing" or "orthogonal" to the access arrow. These two "arrows" depend on each other (in fact the permission exchange is triggered by the access request and the permission exchange carries user data); and the user access exchange depends on the permissions given. Nevertheless, these dependencies do not mean the two exchanges are the same or even that they occur in the same "channels." As authentication and authorisation mechanisms become more complex and generic, these exchanges become distinct and separate; in fact, they use also different technologies and protocols to establish communication.

A wider picture of these exchanges in the organisation will have to make abstraction of the details of the exchanges, while retaining the essence of the matter: how permissions and user management

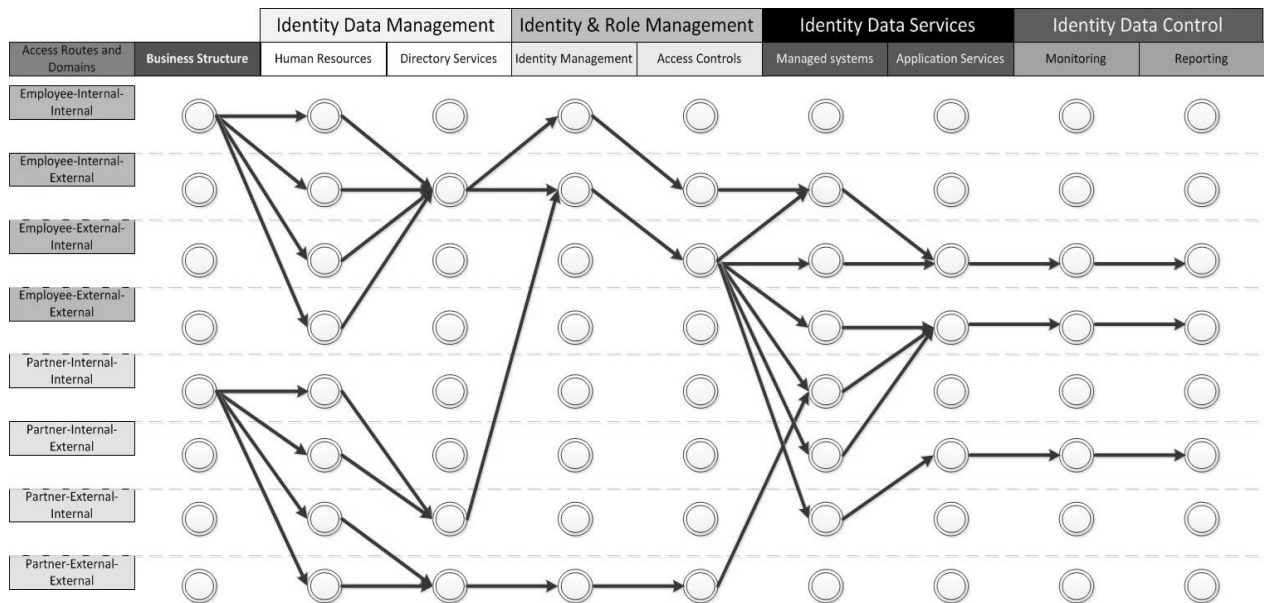
enable user access. Let us consider now an image of multiple user access routes to resources from inside and outside the organisation. This will allow us to show also how user access information "flows" across the "layers" of the Identity management architecture.



Simplified Permission interactions (© C.Trigoso 2012)

This diagram shows the permission (authorisation) interaction for various types of users, for example employees accessing internal resources. In all cases, Identity and permission information moves through different layers, beginning with the organisational structure depicted here as "business structure" under the brown label on the left side of the diagram. The other layers are Identity Data Management (Governance), Identity and Role Management, Identity Data Services and Identity Data Control. What we describe here in several steps represents the "vertical" red arrow in the previous diagram (Expanded User Access Interaction).

The experienced reader will see immediately that the "flow" shown here is extremely simplified, because it assumes that each user type (the green labels on the left) have a single path or direction of flow, until the information arrives at the last stage (Reporting). In reality, these data flows are more convoluted, because they have grown with the organisation and are the result of a multitude of partial solutions and isolated technologies. The real picture is more or less like this:



Typical Permission data interaction (@C.Trigoso 2012)

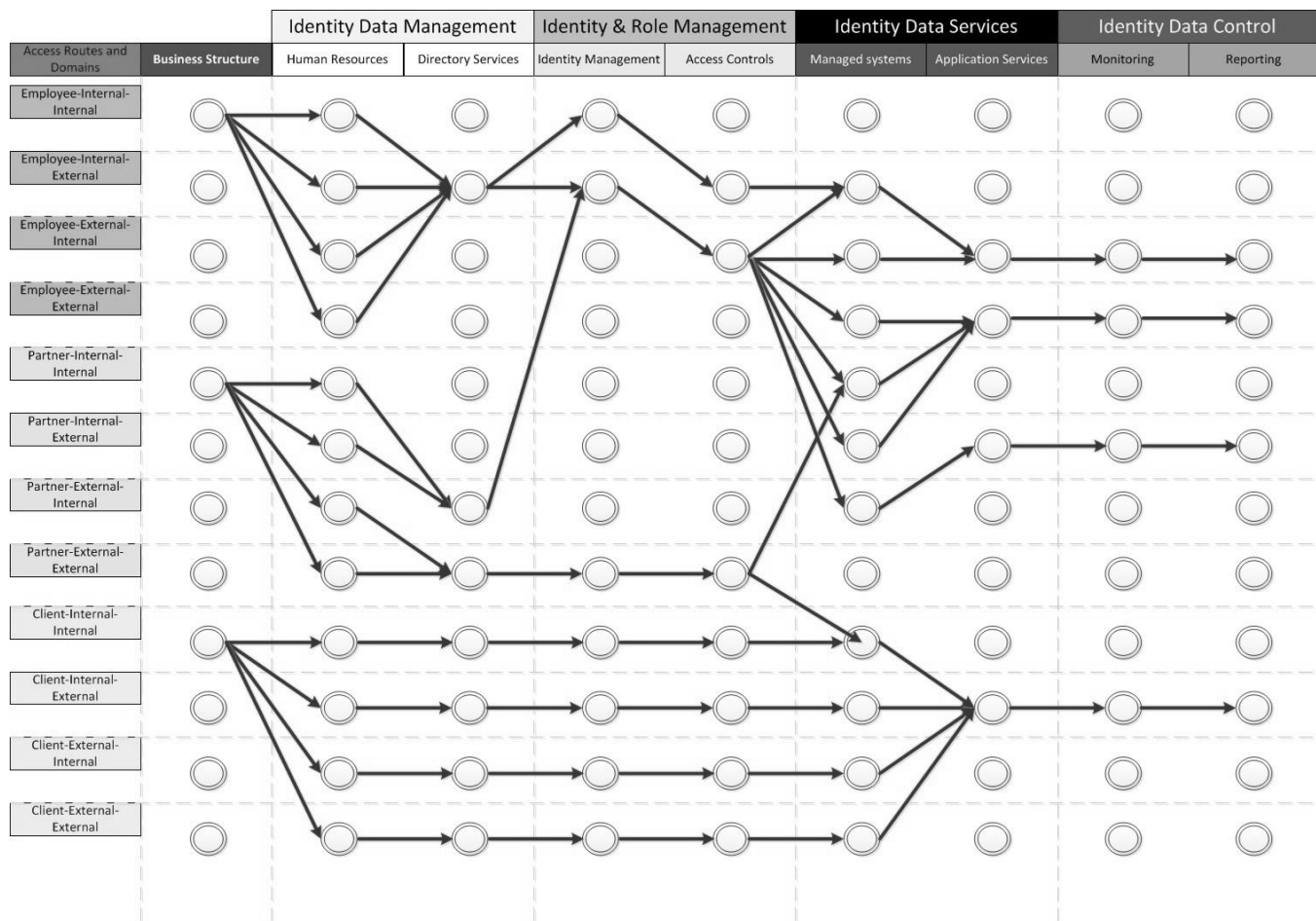
In this case I show also additional user types (external or third party users), but also the fact that user types are managed in a variety of ways and data is mixed and moved from one layer to another in more or less complicated "paths." An even more detailed picture of the situation or real-world organisations would show that several user types are not managed at all, or that if these are managed, not all layers are in place, so that, for example, there is no monitoring or reporting in the user environment. Overall, this picture should work only as a motivation to consider the subject of Quantitative Identity Management from a new angle.

A factor must be added to this view: The increasing and overwhelming importance of external users in organisations. As the traditional organisational boundaries disappear, the types of users become more numerous, and the range of valid user access routes blurs the distinctions between internal and external users. The full scope of user types is usually wider than this summary list:

- Owner
- Manager
- Staff
- Contractor
- Consultant
- Partner
- Supplier
- Customer
- Federated user
- Visitor

While there are still differences related to the types of transactions these users need, many sub-sets of users in each of the categories have the same access requirements. Sometimes, users previously considered “external” have more access rights than “internal” users. Also, internal users interact with the organisation also as external customers and external users have access to internal information sources in various degrees. This leads to a situation where “enterprise Identity management” cannot be formulated separately from “customer or consumer Identity management.”

This leads to a situation too where the Identity landscape, including all data interactions, is much more complicated. The following image shows an increased number of user types on the left side and a more complex network of interactions. This is obviously only an example and each organisation will have a different set of information routes and actors.



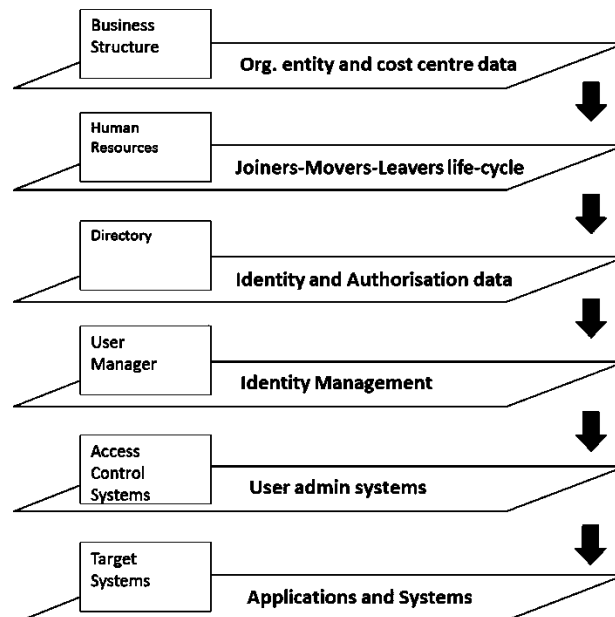
Generalised Permission Data interaction (© C.Trigoso 2012)

If we compare the second diagram in this chapter with the situation depicted above, we need to keep in mind how permission data exchanges act as a "gate" or as an "enabler" for user access to resources. In the more complex diagram, we should now look at the Managed Systems and Applications, which represent Resources accessed by the users. These are shown in two columns under the label "Identity Data Services." We see there two types of resources: Managed Systems and Application Services. It is not important now to explain these in more detail, but just to keep in mind that users request access and eventually work on these resources (Systems and Applications), and all productive work from their

side is done at this stage. It is easy to see that if the data interactions that move across the diagram from left to right are not efficient, limited, or non-existent, business processes will be disabled or at least made less effective and costly.

The normal case in an organisation with an inefficient permissions data "flow" (in reality a series of bi-directional interactions) is that "the job gets done" anyway, although with serious delays and absorbed costs arising from these. Users that are not "gated" or "enabled" via an Identity management solution still get access to the resources they need, but at great cost. Afterwards, these users remain attached to the target resources, and start amassing permissions, which in turn become a Security problem for the organisation. This is how Security problems arise from the lack of efficiency in Identity management.

If we consider these problems only from the standpoint of the Protection paradigm, we would be looking only at the effects and not the causes. For sure, excessive or lacking permissions at the Resource level (Systems and Applications) must be seen as Security issues, but the underlying problem is non-existent or underperforming user management. This conclusion can be visualised if we take another view of the informational exchanges in the organisation. An idealised Identity data "flow" – even if it is not mature and rationalised-- looks like a series of steps and interactions:



Identity Data "Flow" example

I use this image to explain how user management rationalisation and streamlining has a direct impact on productivity and business performance. At the same time, this shows the "movement" of data from the identity repositories at the top to the applications and systems at the bottom is also a performance problem and needs to be addressed with more or less standard methods used in common data management.

Identity Information Logistics

It is convenient to change the language we are accustomed to, and consider Identity management as a type of Information Logistics. There are several definitions of this area⁵ but there is agreement among the specialists, considering that the aims of Information Logistics are:

- To generate the correct information product
- ... at the accurate point in time
- ... in the correct format
- ... in the correct quality
- ... for the intended recipient
- ... at the right location

These goals agree point by point with the aims of an Identity management programme, which should aim at generating the correct identity information (accurate, in the correct format, of acceptable quality) for the intended recipient (the user) and in the right location (in the managed application or system and in the correct geographical or business location).

According to Apelkrans and Abom,⁶ "the value of the information is dependent on the time and place, hence we introduced the value function V [where I = input and O = output]."

- $V(I) = V(I(\text{time, place}))$
- $V(O) = V(O(\text{time, place}))$

The authors add: "The desire is that ILP [Information Logistics Process] is a value-adding process which means that $V(O) > V(I)$. During the ILP process time and even place can be changed, so information can be obsolete, distributed to the wrong place, etc. in global environments, the partners can move around, be substituted, etc. The problem of wrong place distribution is especially true for mobile workers. In the same way, the desire is that ILP shall be a quality increasing process. If we can find a way to measure quality we denote the quality function by Q : $Q(O) > Q(I)$."

For Identity management, this approach would mean the incoming information, for example Human Resources database records, is processed to become authentication records to facilitate user access to business resources. The output value then is higher than the input value as expressed by the Apelkrans-Abom formula. We see here a direct way of associating informational processes with a general notion of value related to the process itself, i.e. the exchange of information. In this case, we do not rely on ideas of either "intrinsic" or "relative" values, but on the quality and quantity of the exchange of information.

Other researchers have proposed more complete formalisms. These should be considered as we progress in the adoption and perfection of Quantitative Identity Management. Of particular interest is the model introduced by Vaidotas Petrauskas in 2006.⁷ Petrauskas focuses on "a three layer system where information flows connect material flows with decision-makers" and where the goal is to find a

"fit of performance and cost." His approach considers three "information flow parameters": path, time and cost, which are defined as follows:

- Cost (of current/alternative process)
- Time (speed of information transfer)
- Path (number of flow network elements)

These parameters correspond to a "network flow" with information feedback. Information "moves" from a set of sources to a set of consumption points and passes through several administration and aggregation points, in a way similar to the Identity data flow model represented on page 123.

- **Material points** = $M_1 \dots M_m$
- **Registration points** = $R_1 \dots R_r$
- **Data stores** = $S_1 \dots S_d$
- **Processing points** = $A_1 \dots A_p$
- **Decision points** = $D_1 \dots D_d$
- **Feedback** = $F_1 \dots F_f$

The "path, time, cost function" $(P, T, C) = x(y, z)$ is obtained by estimating the complexity of the nodes in the network and how the "flow" is implemented:

- Measure of complexity:** $y = \langle M, D, R, A, S, F \rangle$, which results from the combination of material points, registration points, data stores, processing points and feedback channels.
- Structure parameters:** $z = (z_1 \dots z_m)$, which depend on the number of paths across the different layers of "points."

Following these definitions, Petrauskas suggests the goal of information management in this context is to find a function $f(P, T, C)$ which tends to a minimum value. The goal is to determine the set of paths and the level of complexity that will ensure the maximum efficiency in terms of information movement from the sources to the consumption points. Just considering the formal approach presented by this author shows the parallels with Identity data management, although the "consumption points" in our case are the systems and applications managed by the Identity solution and not "decision-makers."

To complement these approaches to value and efficiency, it is also important to study the general form of the problem. What is the optimisation model that is most appropriate for identity data exchanges? From experience, we know the Identity management "problem" is of an organisational nature (as I have described in several sections of this book). By organisational I mean structural and functional and not only "cultural" or "subjective."

This emphasis on structural and functional factors is there to counterbalance the usual inclination to see Security and Identity management problems only as issues of technological "improvement." Nevertheless, we must also understand that even in the most mature organisations, Identity management is never optimal and its defects cause problems elsewhere in business operations and in other areas of Information technology.

Network "flow" analysis and a rational approach to information logistics --as pioneered by researchers like Apelkrans, Abom and Petrauskas-- will help to improve the situation. Nevertheless, while putting more emphasis on the goals of information exchange performance and efficiency, we should not be unduly optimistic, because there is also circumstantial and formal evidence that there is no known solution for Identity data management problems. A brief look into the mathematical complexity of the problem will help us adopt a moderately optimistic approach and focus not on mechanical optimisation of data processing, but on those improvements achieved through organisational change.

Before addressing the general form and complexity of the problem, I think it is useful to understand how Identity management issues affect the organisation and IT operations as a whole. Building on previous chapters in this book, where I showed the persistent problems in Security and Identity management, let us now consider the typical situation in an IT Department charged with a number of projects. In that context, failure and financial loss is not only caused by errors or problems within each project taken separately, but by the interaction between projects. As described by Ashok Mohanty,⁸ "In a multi-project execution department, projects arrive at intervals defined by business initiatives, and not by plans issued by the IT department itself. The schedule is then prepared considering type of work, duration, delivery dates, value and relevance for the business." We know that project execution deviates from the intended schedule, and, as pointed to by Mohanty, project expediting is a "control action" for bringing projects back to schedule. In this context, for each project, the usual parameters are the expected start time and maximum allowed duration. It is usual to add a "margin" to these parameters, allowing for delays and problem management. To assess project performance, a common quantitative model would employ the following variables:

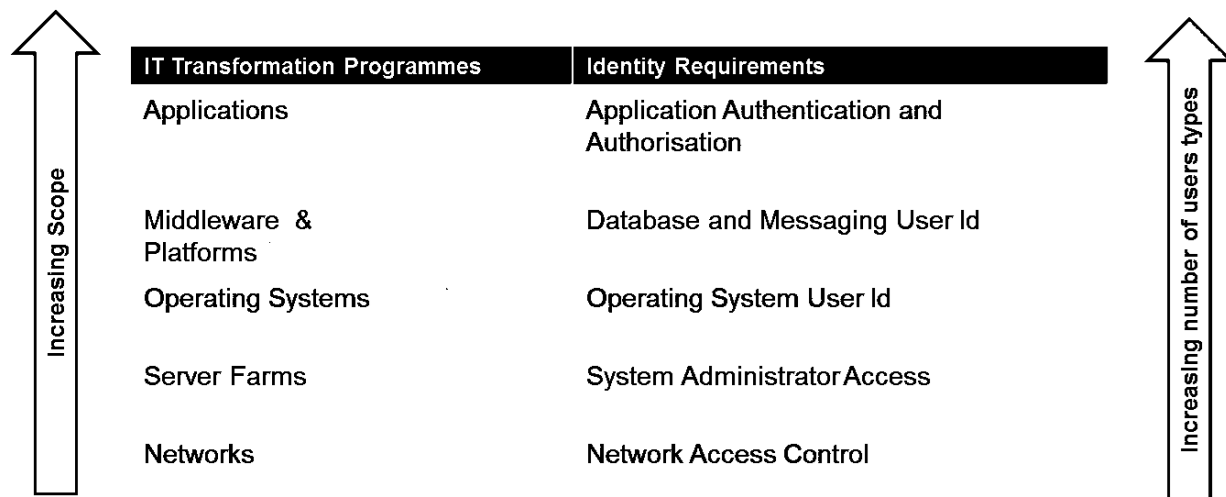
- Actual start time
- Expected duration
- Standard deviation in expected duration
- Maximum allowable finish time
- Fraction of project completed at time of review
- Estimation of completion time
- Value attached to the project finished at the estimated time
- Effectiveness of the index of expediting
- Percentage of time spent in delivery work of solutions (chargeable hours)
- Percentage of in-flight projects within target cost variance level
- Percentage of completed projects within target cost variance level
- Percentage of project backlog in man days
- Delivery cost, schedule, quality and scope

Mohanty formulates the standard calculation that follows from this approach: "If a project starts at expected start time t and takes expected duration d , it is completed at **point A**. However, due to delays, the project may start late, at time $t+x$. The rate of progress may also be slower. At time t the project has progressed to point **B**. If the project progresses at this rate, it may be completed beyond the termination date." Although trivial, this description is nevertheless precise, and is exactly the reasoning we use in everyday project management. Every IT project manager will recognise that the main category of impact in his or her work is what can be classified as "project delay."

When correlating Identity management with Security and other IT project delivery issues, we rarely understand how these affect each other. In particular, there are no studies as to how the limitations and delays in Identity management slow down and increase the delivery costs in other areas of IT Programme delivery. This is an area still awaiting detailed study, but it will be necessary to overcome the persistent tendency of the IT departments to implement technologies lacking in Identity management capabilities.

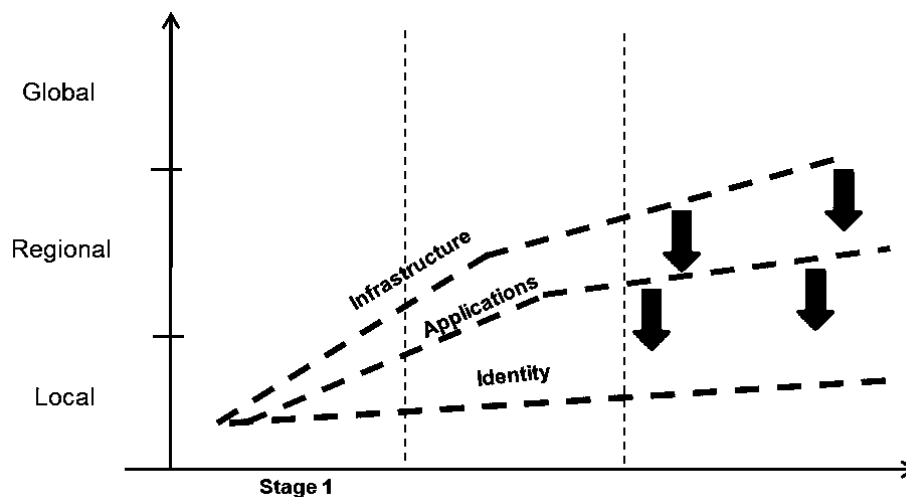
This resistance to an integrated view is obviously negative, but it is also evidence that technology specialists tacitly understand their methods are unable to cope with organisational complexities, so they stay away from Identity issues and deliver even more fragmented solutions instead. Business teams and Security leads need to understand though, that if we start seeing Identity management as a Performance problem, then the impact on other areas will become clear. My experience shows the main impact of lacking or non-existent Identity solutions is on the overall duration and cost of Business and IT transformation programmes. The following discussion illustrates what I mean by this.

The impact of Identity management issues can be seen in all types of public and private entities, but it is especially visible and damaging in global organisations. The main cause and effect relationship is the increasing complexity of user types and applications across the organisation's divisions slows down systems integration and leads to fragmented and costly workarounds. This in turn affects the delivery of shared systems and applications. The more the organisation progresses in the IT transformation road map, the more challenging it becomes to manage Identities.



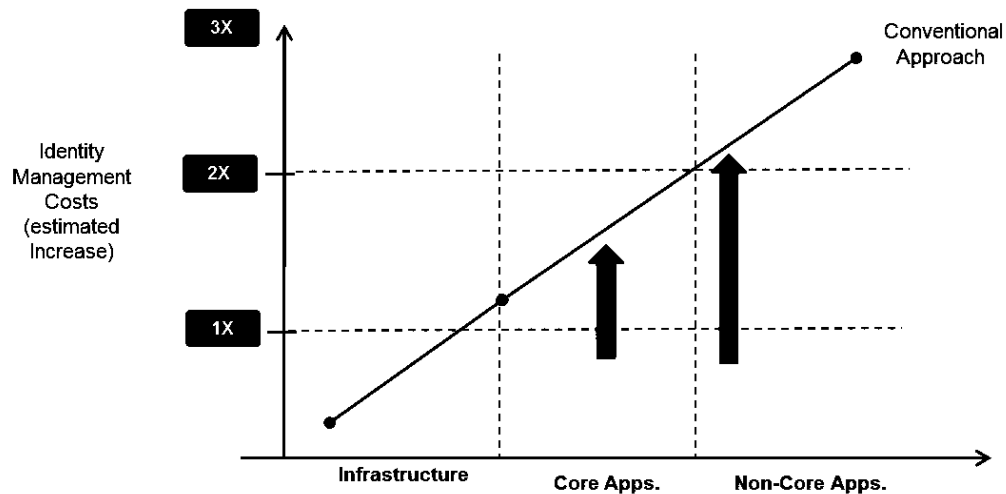
Increasing Identity requirements in global IT programmes

Increasingly, the lack of Identity management capabilities slows down global transformation programme delivery. Infrastructure integration progresses initially at a more rapid pace, given the relatively small number of technologies and targets involved, allowing it to achieve its integration levels faster. The gap in terms of integration and scope increases with time so that Identity becomes a blocker and slows down IT transformation.



Identity management slows down other IT and business areas

Identity costs expand, while catching up with other programmes along several years. Costs expand continuously as the organisation progresses from Infrastructure to Non-Core applications (eventually local applications).



Identity management costs expand in a multi-year period

Though not researched at all, given the strange status of Identity management in Security and IT in general, it is enough to give a little attention to these problems to understand there is a direct relation between the efficiencies or inefficiencies of Identity data "flows" and how these impact other areas in the organisation.

In conventional Security and IT practice, the intuition of performance and effectiveness is embedded in several aspects of our advice and solution design. We also approach Identity management and access control with a series of pre-conceptions of what is considered "better" or more "valuable" for the organisation. Sadly, this is not enough, as one key aspect of our advice should be how to increase the performance of Identity data exchanges. While immersed in the risk-based approach and the mechanistic view of Information, we are unable to articulate this or even to think about the problem. Although sometimes we distance ourselves enough from the "Protection" concern, and start speaking about the "efficiencies" that are to be found in Identity management, we remain still unable to think about Performance.

Therefore, instead of working on minimising the value of the Path-Time-Cost function --as needed in the Petrauskas model-- Security and Identity practitioners and experts advocate a mixture of technologies and forms of automation. Under the spell of the mechanistic paradigm, we assume that the key benefits are not related to organisational structure and operation from the organisation, but to the lack of some "tools" or "technologies" that will "help the IT department" cope with their obligations.

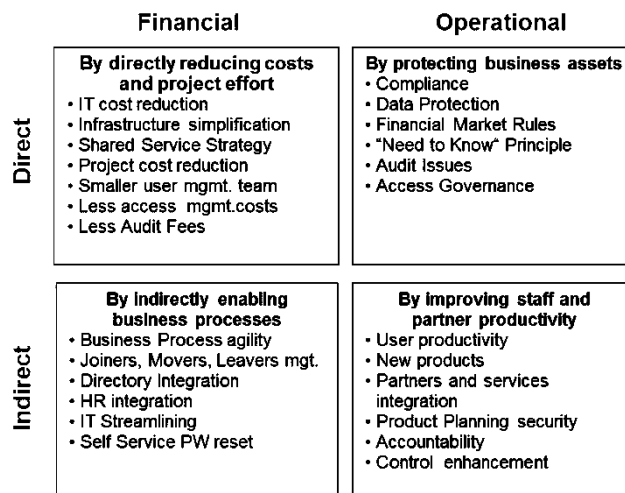
This happens, even though we know well that Identity management solutions create mainly indirect and non-financial benefits. These benefits are quantifiable but can be measured only in the

organisation as a whole, i.e. in the correlation between Identity management and Business and IT programme delivery. Therefore, the emphasis on "Protection" and automation paradoxically distances the Security and IT practitioners from a proper quantitative approach.

Quite differently, in this book I show the main benefits come not from automation, but from the enablement of Business and organisational transformation. In other words, as indicated at the beginning of this chapter, the benefits come from the "gating" effect of identity data interactions and not from the automation of these flows themselves. This is the fundamental claim that is at the centre of the Quantitative Identity Management view.

Years of frustrating experience have led most Security experts to believe that Identity management benefits are indirect and difficult to measure. My suggestion is that these difficulties –while real—are caused by a lack of understanding that Identity data processes are bi-directional and consist of exchanges, and therefore can be measured only by their impact on the processes that are enabled or disabled by them. This is what I called the "gating" function of identity data exchanges in an earlier section of this chapter. Corresponding to this, a view of Identity management as a performance problem will finally allow us to have a quantitative approach where before we just had intuitions.

The following diagram shows the variety of impacts and areas where Identity management solutions have to be measured:



Identity management impact areas (@ C. Trigos 2010)

As we discussed in previous chapters, Identity systems are notoriously difficult to implement, upgrade, and to validate as investments. So, several questions arise: What should be measured to assess the "current system" in a particular organisation? If roughly ¾ of the benefits are non-financial, how should we estimate investment returns? If non-financial benefits cannot be measured, should an Identity management investment decision rely only on expected financial returns? In addition, if we limit

ourselves to the estimation of financial benefits, what are these exactly? Moreover, how do we assess the distinction between direct and indirect benefits in any case?

The Quantitative Identity Management approach I propose in this book begins by first representing and analysing the Identity systems—both the current and the proposed solutions—as networks of Identity data exchanges. The networks are composed of Identity sources, processors and consuming entities, as well as entities acting as authorising, validating and managing parties. While it is not new to formulate Identity systems as workflows and business processes, this approach goes further:

- It allows for decentralised workflow models including user driven or user started Identity data management
- It integrates security criteria about assurance (security information quality) and not chiefly about subjective "risk" assessments
- It introduces the notion that business services and projects are consumers of Identity data
- It moves from a defensive position, where Identity management is done to remediate and comply, to a trust management stance where the emphasis is on performance and data quality in support of business projects
- It puts IAM finally in the context of Service Oriented Architecture and Security as a service, while it does not assume a closed organisational context
- It separates the overall quantitative performance analysis from considerations about locating the participant entities, which can be either in or out of the organisational boundary
- It subordinates non-quantitative targets to hard targets of data availability and quality, including demonstrable account provisioning and de-provisioning (termination)
- It subordinates weak measures of user productivity and enablement to data availability and integrity measures (are users provisioned in time?)

In addition to that, a quantitative approach, when "Identity becomes data," firmly centred on quality and availability, can address simultaneously the goals that I highlighted for any Security management programme:

- Adapting the organisation to a reality where there are more and diverse users outside than inside of the "boundary"
- Adopting a multifaceted view, where the organisation is a partner in the Cloud and not the only or main Identity provider
- Enabling business management to assert quality and cost control through efficiency comparison of services
- Enabling the organisation to estimate the impact of Identity data exchanges on IT programmes and transformation
- Overcoming the one-sided risk-based approach
- Preparing the organisation to the period "after" the Cloud, when IT services are consumed on a utility basis
- Revealing the nature of cost variations between services provided by suppliers

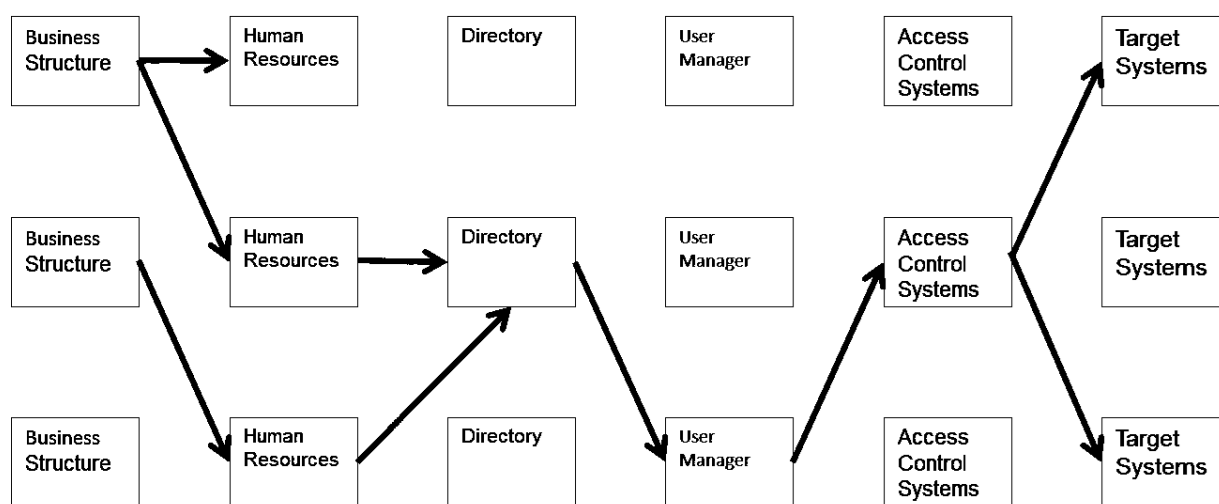
- Supporting the transformation of Security and Identity management into normal business operations and align the investment patterns with other areas of financial management
- Supporting the transition of organisations to Cloud infrastructure and services

On those lines, still following our intention to reveal the "form" of the problem and avoid an "optimistic" approach, we can now turn to a deeper assessment of these guidelines.

We need to consider first what type of optimisation problem we are facing. If we take the previous insights into the layers of the Identity architecture, the concept of the value function, the formal Path-Time-Cost model, and the interdependence of IT projects, we can continue this investigation productively.

A key insight is provided by the work on "system design" by Bahill, Chapman and Rozenblit.⁹ I will follow here in particular these authors' idea that engineering systems design is a so-called NP complete problem.¹⁰ By "systems design," Bahill and his co-authors mean the process of "translating the customer's needs into a buildable system design," a task which "requires selecting subsystems from an allowable set and matching the interfaces between them."

Bahill summarises the design task with the term of Systems Coupling Recipe, which is the graph or network formed by all the subcomponents of the solution. A systems design problem, as the author explains, can have many solutions but each of these will be some form of "connectivity" (i.e. a network) between the components of the system. A diagram illustrates this as applied to an Identity management environment:



Potential connectivity for Identity subsystems (based on Bahill, 2009)

This shows essentially an Identity management solution, where--after assessing the needs of the consuming services--we propose a series of chained systems and processes to cover those demands. When there are no services capable of supplying authentication and authorisation, we propose new systems or re-engineering of existing capabilities to obtain those results.

As Bahill explains, "NP-complete" is the name of a class of problems for which there is no known efficient deterministic mathematical (algorithmic) solution. All known algorithms for solving these problems have the property that as the problem size increases, the number of steps necessary to solve the problem increase exponentially. Problems that have efficient solution algorithms can be solved in several steps that increase at a slower rate; that is the solution complexity can be managed in a reasonable number of steps.

Bahill gives as example the sorting of a list of numbers—an operation that can be finished in n^2 operations. If we have 10 numbers to sort, it would take at most 100 operations to perform the sort. A hard problem is different in that its size is in the exponent. Bahill gives as example an exponential problem where "the number of operations quickly exceeds the capability of any machine to compute a solution. For example, if there were a machine that could do 10^{12} operations per second (none yet exist) and there was a problem that required 10^{20} operations, it would take 10^{20-12} or 10^8 seconds or more than 3 years to solve."

In systems engineering –following Bahill's approach—the design problem can be described by stating the input/output relationships, the design constraints and the performance and cost figures that are relevant. For a given set of subsystems available to build the solution, a possible network of components can be configured that satisfies the given constraints. Bahill suggests the key is to aim at target values, considering there are no perfect solutions, but also that no definitive formula can be found.

Bahill and his associates compare the system design problem to the famous "Knapsack Problem."¹¹ Bahill writes: "the engineer can find a combined system such that the constraints of performance and cost are simultaneously satisfied. But this would be equal to satisfying the Knapsack Problem, which is NP complete by definition." And later he remarks there are algorithms to obtain good solutions "within a few per cent of a theoretical optimal," but a proper engineering approach is to replace the goal of maximisation with the goal of "satisfaction of constraints," and "find a course of action that is good enough." Bahill goes on to say the engineer must ensure that the customer does not require optimal solutions because these are unreachable.

This introduction to the engineering approach should be enough to show the parallels with the Identity management design task. In our area we also have to "find the shortest patch" and the "lowest cost" for a solution." Each of these challenges can be solved in reasonable time, but the complexity comes from the fact that we have to find simultaneously the shortest path, the least costly implementation, and the most effective allocation of users to resources and vice-versa. It is important to note the real-world Identity problem is much harder than the system's engineering task, because we have to deal with a changing, badly defined target, and many times do not have the advantage of a specified product or result. If we look again at the four layers of Identity management architecture and the data exchanges discussed in the first sections of this chapter, we will be able to describe the "form of the problem" more closely now.

Identity Data Management is “NP-complete”

It will be visible that as the problem size increases, the number of operations needed to compute an optimal solution expands rapidly making the solution "hard" or "unknown." Eventually, the solution has to be deemed "unreachable" in a reasonable time and we speak of problems where the solution is only "approximate." That is exactly the case of Identity data management, especially in large (more than 50 thousand users) and global corporations (with many locations, data regimes, and different business processes). In these cases, the combination of the different agents and entities in the identity data layers creates an unsolvable problem. We need to consider the whole picture to assess how difficult the task is:

- The sets of all possible items (the identity data entries)
- The size of individual items (the identity data structure)
- The value of each individual item (value associated with each data record)
- The data dimensions (data stores, data entries, etc.)
- The value goal (including quality and availability goals for data distribution)
- The allowed technology (identity data management technologies)
- The system interfaces to other systems (consuming services and projects)
- The cost of individual subsystems (cost per user and per transaction)
- The performance of each individual subsystem (for example directories or gateways)
- The allowable costs of a system (budgeted or contracted value)
- The required overall system performance (overall service levels expected by the client)

Once we collect these parameters, a strict analysis process would lead us to a "map" between the elements of the problem (users, managers, processors, controls, and targets). In the terms of the "Knapsack Problem," this would amount to mapping the "agents" to "positions" and then to managed systems or "resources." This represents then a "graph" or "map" of the different layers of elements that intervene in the problem. For this kind of problem, we would have a "multipartite graph," drawn from a series of entities:

- **A set of elements** $A = (a_1 \dots a_n)$
- **A set of processing points** $P = (p_1 \dots p_m)$
- **A set of targets or resources** $R = (r_1 \dots r_x)$

The "effectiveness" of a combination of the entities designed as A, P, R, etc. will then depend strictly on our ability to satisfy simultaneously the goals of time, cost and performance. Engineering practice recommends though, as explained by Bahill, that "The first implication of the System Design Problem being NP-complete is that humans cannot design optimal systems for complex problems. And computers will not be able to bail us out, because computers cannot design optimal solutions for complex problems either."

Identity management is such a problem. In a real-world Identity management context there are many more classes of entities in interaction than in the elementary example given in the previous paragraph, or those that can be found by researching on NP problems in industry and commerce. We have to deal at a minimum with four classes of entities and 12 classes of internal and external access routes. In addition to that, the "resources" and "targets" are not simple but very frequently also composed of

several subsystems with different and sometimes contradictory requirements. It is evident that the solution constraints are more complex. Besides that, the allocation problem is not completed with a single distribution of users to resources. Indeed, the user to resources mapping will change continuously in time as the organisation expands, merges and adapts to changes in the markets.

In any case, it is fitting to see the Identity management problem as the result of many interacting information exchanges, a "network of exchanges," which can be expressed as a "systems design problem," i.e. as an NP-complete optimisation task. In considering this, we should have a "hard" look at the conventional approach to Identity management based on workflow and provisioning tools, as well as "role mining" software. The truth is these tools can solve parts of the Identity management problem, and only for a limited time. So, when we progress towards quantitative approach, it is essential to aim at achievable solutions which do not highlight automation, but satisfy client requirements and organisational goals. A mechanistic, "automation" solution for example, will always fail to manage complex external and internal scenarios, whereas an organisational performance approach will instead succeed by abandoning the illusory goal of "managing" all the users that access business systems.

Adopting the view that Identity Management is a performance problem does not mean then that we should adopt the mechanistic approach just because we learn from systems engineering. The best exponents of engineering (and Bahill is one of them¹²) actually endorse a view that takes us away from computer-centric solutions. My point is not only that automation solutions will be eventually not satisfactory in the new Identity landscape, but also that we need to redefine the Identity management problem altogether. Instead of aiming at the "solution" of the combinatory explosion between users, sources, processors and resources, it will become clear that it is essential to aim at the reduction of the combinatory, i.e. the reduction of layers and subsystems to the essential ones, and reducing complexity of the data types managed. On the other hand, a reduced set of layers and data types does not mean a reduction in performance or the ability to deliver, but ensuring that good quality, standardised information is made available across all targets, while the systems and applications serve users the available information following their own consumption criteria. In other words, Identity data should become a service, a utility within the organisation, and should not be governed as one more "silo" in the already problematic IT world solutions and tools.

Performance Measures

Following the focus of IT and Business alignment after the IT Boom had passed in the early 1990s, professionals started to use measures of value that were closer to normal business criteria. These were introduced both to justify technology investments and to evaluate the result of technology adoption. The most common measures were those of effectiveness, efficiency and productivity, defined as follows:

- effectiveness = actual output times 100% / expected output

- $\text{efficiency} = \text{resources actually used} \times 100\% / \text{resources planned to be used}$
- $\text{productivity} = \text{outputs} / \text{inputs}$
- $\text{expected productivity} = \text{expected output} / \text{resources expected to be consumed}$
- $\text{actual productivity} = \text{actual output} / \text{resources actually consumed}$

In this context, IT and Security professionals started speaking about "value maximisation" of investment, and looking for measures that would reflect the contribution of IT to business value. For example, we were introduced to the ideas of:

- Speed-to-market – meaning fewer delays, removal of bottlenecks, and increase of productive days
- Reduced cost-to-serve – including fewer overruns, proactive use of lower cost delivery options, and increase of utilisation rates.
- Reduced overheads – including reduced project management and reporting costs, and reduction of wasted management time

Identity management introduced its own measurements, of which we can cite the most important ones contributing to the complexity of the task:

- Number of accounts
- Number of groups
- Number of roles
- Workflow branches
- Account usage statistics
- Password reset statistics
- Number of authentication tokens
- Number of authentication requests
- Number of authorisation requests
- Number of escalation of privilege requests
- Number of access requests per approval
- Number of steps for account lifecycle
- Identity repository size (including number of groups and roles)
- Ratio of requesters to approvers for a given target
- Number of accounts per user
- Authentication claims (attributes)
- Personal Identifiable Information claims (attributes)
- Potential and actual locations the workflow can provision to
- Provisioning paths (routes traversed by identity claims)

In these respects, Identity management solutions aimed at reducing complexity and complementing IT Service Delivery and Support. The common assumption was that Identity management technologies would increase productivity and efficiency enabling user access to applications "at the right time." While it is true that an identity management technology could handle an almost unlimited number of users, far greater than the "largest organisation," a crucial point was missed in these calculations: the combinatorial complexity described in the previous section. So, organisations adopting Identity solutions only gained a fraction of the expected results and could not reduce costs rapidly, nor integrate new business initiatives as desired. It has not made big headlines but major organisations in

the world responded to these failures by abandoning Identity management technical solutions and focusing instead on urgent requirements around regulatory compliance.

Then around 10 years after the introduction of complex Identity automation solutions by major technology vendors, the market began to abandon these technologies. When the Identity management market consolidation seemed finished with the creation of four or five large vendors in the market, suddenly several of these disappeared from the scene and new challengers surged with more focused initiatives. Complexity defeated the drive to automation, while simultaneously organisations transformed into networks of organisations, creating a more diverse landscape of identities that was not anticipated by the technology.

Now, all the primary goals of our speciality, like increasing business agility, reducing project efforts, accelerating system implementation and eliminating security issues can be and still are attainable, on the condition that we abandon the idea that an increase in performance requires an increase in automation. We still need performance indicators like the "average time to perform" or the "elapsed time between service violations," but these have to be achieved with an effort composed fundamentally of organisational transformation and not automation. People say that organisations have large expenditures in manual user management processes, including high head-counts for user administration and long delays for user on-boarding and off-boarding. Lengthy provisioning processes are mentioned as a case in favour of management automation. On the other hand, from the vantage point of our understanding of the complexity involved, we can see that these manual, slow, custom solutions are the way organisations cope in the real world with a difficult problem that resists automation.

In other words, the reason organisations have fragmented processes for managing physical and logical access, and why they perform user management in an ad-hoc manner is because the problem itself is ill-defined and informational exchanges are too complex to reduce to an "industrial" proposition. There must surely be an exit route from this difficult situation, but it requires first a revolution in thinking.

Forms of Identity Management Optimisation

Once we adopt a quantitative approach to Identity management, we can see several forms this may take, depending on the maturity level of the organisation. Here is a summary of these forms:

- a) Standard: In this case, Identity management data exchanges can be seen as a multi-source multi-sink network flow, where the goal is the maximisation of data "flow" between the sources and the sinks. This is equivalent to finding the shortest paths for data to the end consumers. This form of optimisation corresponds to a general idea of user access enablement, and input into project delivery, with little regard for the quality of the data or the complexity and changes of the "flows."
- b) Extended: This is another basic form of optimisation, which can be understood in terms of the internal completeness of the Identity management processes. Calls for maximum integration of data, standardisation and reduction of processing teams represent an effort to reduce the complexity of the network in addition to finding the shortest paths.

- c) Valid or Compliant: This type of optimisation implies a complete set of internal and external processes and the matching solutions. We can say that here the focus is on the inclusiveness of the controls, aiming at accounting for all the access routes to shared and non-shared resources. In this case, I believe we can speak too of a "maximum communication" model where all data exchanges are in scope.
- d) Secure-complete: This fourth form of optimisation requires a maximum layering both in the sense of division of labour and types of users/services. This can be realised with the four architectural layers that we discussed in this book. The key difference is there is a deliberate process of differentiation and communication extending across the network, including extensive organisational transformation.

In all cases, even within a conventional context, these four optimisation approaches highlight the essence of Quantitative Identity Management:

- The inter-dependence of the identity data exchanges
- Bi-directionality of identity data "flows"
- Homogenisation of internal and external identity data
- Dependency of project and programme delivery on user enablement

Simultaneously, assuming the nature of the problem is one of data management optimisation allows us to see interesting links with traditional engineering, data integration and transport scenarios:

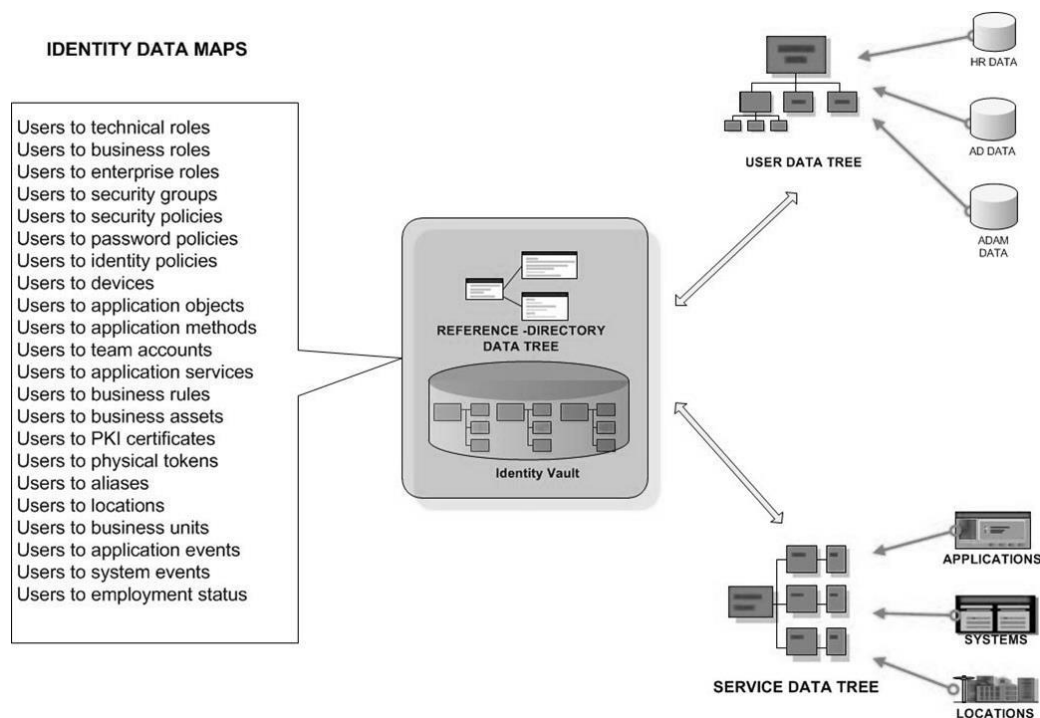
- There are similar communication costs for integration solutions
- There are economies of scale for shared links between different targets or systems
- Loading and unloading data is similar in the sources and points of consumption

In general, this leads to a "hub and spoke" model, similar to the one used in transportation economics due to its large advantages for business rationalisation. Eventually the hub and spoke model materialises by the force of economic and social drivers, independently of the preferences of the IT departments. In fact, what we see in the nascent Identity management Cloud-based services is nothing but the development of this model.

So, we have formulated the problem in terms of information exchanges and bi-directional data movements. We have started to think in terms of how much information is produced by the user and how much information is sent back to him or her. And we understand now that information flows are correlated and co-dependent across the organisation, that they form a network, and that we can have measures of performance not based on automation.

If we look closely at the normal organisational requirements, Security and Identity processes depend on the association between users and resources. A key observation is that one type of information – Identity data moving across the organisation—acts as the "gating" or "controlling" function in the access of users to resources. This conditions the productivity of the users and the general results of the

business. These information exchanges constitute a series of mappings, which usually can be classified as a data warehouse model. The following image shows the overall structure of such a database, which I suggest must be the core of a Quantitative Identity Management solution.



Identity data mappings (@ C. Trigoso 2006)

While these mappings can be diverse, all of them have in common that they are rooted in the natural person or individual that is associated with the organisation as either an internal or an external user. The implications of this will become clear in the next chapters.

Far from the traditional focus of "centralising" all the information sources, the goal becomes one of simplification without mechanical reduction of complexity. Far from the traditional focus on "automation," the goal is one of organisational transformation and the search for excellence appears as the supreme goal of management. Identity management grows into a Quantitative discipline with new functions and a new division of labour.

¹ Robert L. Phillips, "The Management Information Value Chain," Perspectives , Issue 3 <http://www.talus.net>

² Phillips elaborates: "The usefulness of the information provided by the Management Information Value Chain is determined by its effect on decisions. The value added by any management information activity can be derived by calculating the extent to which it contributes to this goal. We can then determine if the value of an activity exceeds the cost of supporting it -- if not, the activity should be eliminated. We can also identify the "bottle necks" within the value chain-areas where more information or more processing would substantially improve profitability. Perhaps best of all, the Management Information Value Chain approach enables explicit cost-benefit analysis of information technology

investments-placing these investments on the same footing as other corporate investments and providing a mechanism for establishing a profitable development plan for management information systems."

³ Compliance emphasis is unsustainable when it becomes a reactive, audit-driven practice instead of being a normal, standardised business practice.

⁴ Nicholas Carr, 2003. "IT Doesn't Matter," Harvard Business Review, May 2003

⁵ For example: Apelkrans and Abom write "By IL we mean exactly ...send correct information to the right people at the right times," Netguide, 2002. See also: Turban: "IL is the information supply needed to perform excellent logistics," 2002.

⁶ See Apelkrans and Abom, 2001

⁷ Vaidotas Petrauskas, "The Use of Information Flow Analysis For Building An Effective Organization," Information Technology and Control, 2006, Vol. 35, No. 4

⁸ "Mathematical model for expediting the execution of projects," Ashok Mohanty, 2011

⁹ William L Chapman, Jerzy Rozenblit, Terry Bahill, "System design is an NP-complete problem," 2001

¹⁰ "A problem which is both NP (verifiable in nondeterministic polynomial time) and NP-hard (any NP-problem can be translated into this problem). Examples of NP-hard problems include the Hamiltonian cycle and traveling salesman problems. In a landmark paper, Karp (1972) showed that 21 intractable combinatorial computational problems are all NP-complete." – Quoted from Wolfram Mathworld, <http://mathworld.wolfram.com/NP-CompleteProblem.html>

¹¹ "Given a sum and a set of weights, find the weights which were used to generate the sum. The values of the weights are then encrypted in the sum. This system relies on the existence of a class of knapsack problems which can be solved trivially (those in which the weights are separated such that they can be "peeled off" one at a time using a greedy-like algorithm), and transformations which convert the trivial problem to a difficult one and vice versa." – Quoted from Wolfram Mathworld <http://mathworld.wolfram.com/KnapsackProblem.html>

¹² See Terry Bahill's web page here: <http://sie.arizona.edu/sysengr/index.html>

8. When is a System Secure?

Systems and “Systems”

It is a problem of the IT disciplines that the term “system” has a strange existence. At first sight, there is a consensus on what a system is, and perhaps the term is one of the most frequent in our literature and oral communication. Nevertheless, when IT experts are challenged to define a precise terminology, it is almost impossible to find a single definition; instead we have many interpretations, all of them unstable and vague, to the point that we can say that the word “system” hides a large disagreement.

Academic computer scientists are not critically affected by this problem, because they are justified in holding a uniform definition of “system” that is equivalent to “computer” or “network of computers.” After all, the computer is their object of choice. Also not affected are those researchers who prefer to study “socio-technical systems,” considering human interaction as an essential component.¹ Quite different is the case of IT practitioners and experts, who rarely rely on academic definitions, but then fail to have appropriate concepts for what they do. My point here is the current confusion should give way to a wider, more complex definition of system, aligned with the “socio-technical” approach.

A good definition –which is compatible but wider than the one used in academia—is that a system is a socio-technical complex. Machines and people interact and determine each other in the organisation. More precisely, machines are both agents and objects in organisational interactions. In an organisational setting, a system is never a machine or a group of machines, but the communication complex that arises from human interaction *through* computers and their networks. Hence, a mechanistic definition of a system will always fall short of reality and remain fruitless. This is because a machine in itself is fundamentally deterministic, but a network of machines acting as a complex environment for organisational communication is by definition unpredictable and non-deterministic. The social communication factors come to the forefront and the system is not a machine anymore.²

In our professions, though, although we decorate our interventions with the jargon of business and organisation management, including “people” concerns, the object is always the machine, not the system, and we land into deep problems that cannot be resolved within such a limited frame of mind. We should not be surprised about this if we insist on a wrong definition. Avoiding this trap is critical to understanding what should be considered a secure system. So far, from the point of view of Protection, a secure system seems to be a secure machine, a “box” with inputs and outputs which can be “access controlled.” Information is either “inside” of the box, or “moves” from box to box, and has to be protected “at rest,” “in transit” or “in process.” Not only all our intellectual focus but also our expectations are determined by this setting.

Against this, some Security experts have called for a more rounded vision of IT Security (as we saw in the previous chapters of this book), but the confusion persists among the majority of specialists. For sure, it is not only Security experts who are confused: this is a general problem of the entire IT Industry, and in fact Security practitioners just do what is expected from them in the trade, which is to “protect information.”

The “system” in this frame of mind is the computer, perhaps the network of computers, and, more recently, the Internet or the Cloud as a technological environment. As the scope grows towards wider and more complex networks, though, the mechanistic focus of the Security practitioners becomes more and more limiting and eventually absurd. The techno-centric focus does make some sense while computers are isolated or more or less homogeneously connected behind the organisational or departmental boundaries: a single computer can still be called a “system” and it can be addressed and protected like a whole entity when it is isolated. Once it is connected to other computers and especially open to the Internet, the mechanistic notion starts foundering, because the number of interactions increases and diversifies. The same person can access information from different machines, and in fact it becomes clear that machines become remote agents for individuals. The mechanistic view is even weaker when we include external or Internet users, who --by definition--- are outside of the organisational boundary. Here the same person can access many computers from many different places, and in many different roles, as well as through an unlimited number of machines. What looked like a “system,” i.e. something having the coherence and predictability of a pack of electronic circuits inside a metallic case, is now a tangle of human relationships where the machines are only the ground where these take place.

Security “for” and “in” the Organisation

In the context of the Internet and the Cloud, even when the mechanistic view still has a role, it is necessary to adopt a complementary stance, that of security “in” the organisation. The conventional techno-centric view is that of Security “for” the organisation, rooted in the idea the organisational network “is” the system. Making an abstraction of the complexities of the network, it is still possible to speak of Security measures that will protect informational assets from external illegitimate agents. This is not enough though, and has been addressed many years ago, for example by Carnegie-Mellon’s Octave approach.³ Properly seen, the organisational network and the Internet create a need for Security “in” the organisation.

This is the first symptom of change, arising from the fact that internal and external access are hardly different in complex networks which have entry and exit points to the Internet. Security “for” the organisation becomes as important as Security “in” the organisation. The first thinks of threats and “attack vectors” that are coming from the exterior; the second starts from the understanding that dangers live both inside and outside of the organisational space. It should be clear that these two views are necessary and coexist for a long time in the computerised enterprise or organisation. The delivery of security “in” the organisation becomes a precondition for the realisation of security “for” the organisation.

Nevertheless, while the two views coexist and cooperate most of the time, there is a permanent level of distance and conflict between these approaches. The view focused on Security “for” the organisation assumes that its function is to provide boundary defences, and to adopt technology-based solutions. As the individual computer stops to exist and the network boundary expands, the IT specialists think of more and more technologies to surround the computer with new walls and other “systems” that will close the gaps and keep the information safe “inside.” This is what keen observers meant—even in the early 1980s, when I started tinkering with computers—when they said that our trade was trying to solve a problem by “throwing a computer at it.” We still do it today.

In a correlated but contradictory position, the view of Security “in” the organisation (or the wider network) has as its primary concern the variety of identities (of users and roles), not of technologies. Security in this sense is the Subjective position, which we have associated in other chapters with the disciplines around Trust Definition and Allocation. This is the ideal position of the business leader, the owner, the strategist, but also that of the group, the organisation, and Society in general. From a different angle, Security “for” the organisation represents the Objective position, which is that of the implementer, the controller, the auditor, but also that of the engineer, the technologist, and IT organisations in general.

When considering these diverging views we see that Identity management is located in the Subjective half of the opposition, more specifically in the area marked by Trust Allocation. At the core of the Identity management domain we find principles of Identity Data Management and Identity Data Ownership, and it is clear even in the present circumstances that these disciplines cannot be reduced to technology. Contrary to appearances and technological trends, Identity management consists essentially of Trust allocation processes when considered at the level of the participants of the process. When considered at the level of the communication channels inside and outside of the organisation, this discipline is similar to the specialities of Information Architecture and Integration.

The correct understanding of this duality (between Data Ownership and Data Integration) will lead to the application of available industry and organisational standards to the Security and Identity practices. For example, Identity management must be supported by Service Oriented Architecture and founded on data ownership and stewardship. The service orientation reflects the (objective) technological component, while identity data ownership expresses the “subjective” side. This duality makes Identity management the Security area most affected by organisational factors, and, in turn, the area which has the highest impact in every aspect of the organisation’s processes and structures.

A purely technological emphasis for Identity management misses the point altogether, because there is no Security without data governance (i.e. Direction), especially if there is no definition of what the organisation wants to keep as levels and spaces of trust. The organisation's policies come first, and the definition of what is a trusted environment is a precondition to all other aspects of Identity management and other Security disciplines.

So, in conclusion, when we speak of System Security, we need to present the whole “case” for our professions, especially for Identity management. A system is secure if and only if the disciplines of Trust and Risk management are effectively applied and complement each other. In the current atmosphere, though, Identity management is blocked, ignored, marginalised in Security analysis and investment decisions, because of the bias at the root of the IT professions. Therefore the opportunities and benefits that it brings are missed.

The Paradigm Shift

Recently Ed Granstedt and Troy Nolan made a good argument for the change in the Security paradigm,⁴ contradicting the current ideology of Information Security. The authors wrote: “A successful cyber-security strategy starts and ends with the mission -- we don’t protect our information for its own sake, but for the sake of the mission. [...] Traditional defense-in-depth approaches to securing autonomous systems are only partially effective. They cannot provide complete security to critical infrastructures. Perfect security is not possible due to the rate of change of cyber-threats and adversaries, the burden of IT security costs, the lack of integration of layered defenses and the limits of the technology used to protect information systems. We need to see network and information security as elements in protecting an overall mission.” This statement may not be original in essence, but the terms used are striking and precise. It is also very important to note the distinction between “security” and “assurance.”

Granstedt and Nolan, using military terminology, dispel the confusion: “Unlike perfect security, mission assurance is an achievable goal. But to reach this goal (protecting, under persistent threat, the important elements of infrastructure that support key mission activities), we must look at the mission holistically, considering its infrastructure, its desired behaviour and the information that underpins it.” By focusing on the mission, which in my terminology is equal to the Direction perspective, technological actions become subordinate and relative to the goal. And it is good to see this in a very present context too: “Advanced persistent threats (APTs) differ from other infrastructure threats by their ability to infiltrate, hide and maintain access to an organization’s data across a long timeline. Once inside, APTs add backdoors, map the infrastructure, harvest account credentials, determine information of value and leak that information. This provides access to virtually all the information, and its explicit knowledge, that lies in an organization’s infrastructure, and the individuals behind APTs work hard to maintain that access.”

What the authors are saying, in their own terms, is nothing else than the need to focus around Security “in” and “for” the organisation. This has to be done avoiding at all cost the view that more technology can somehow guarantee the goals of an enterprise or a government! I cannot but quote a specific point which I share: “In this threat environment, organizations can be compromised by a single vulnerability. The character of the APT is such that traditional firewalls, intrusion detection devices and host-based scanners have difficulty eradicating them. The adversary tests against these defenses, knows their weaknesses and is patient, while seeking to find that single vulnerability. The truth is we

must operate under the assumption that our networks are already “owned” and that no amount of castle wall construction (firewall) or moat building (virus scanning) is going to protect it.”

The authors conclude their article affirming that the perimeter of “defence” is “outdated” and recommend not remaining focused on “inbound” actions (i.e. penetration by external agents). They do not explicitly ask for an organisational approach, and perhaps their final recommendations are still techno-centric, especially when they suggest that Security investments should be prioritised around essential infrastructures to support the organisational mission, but this is an excellent approach and Security experts should adopt it wholeheartedly.

Dereliction of Duty

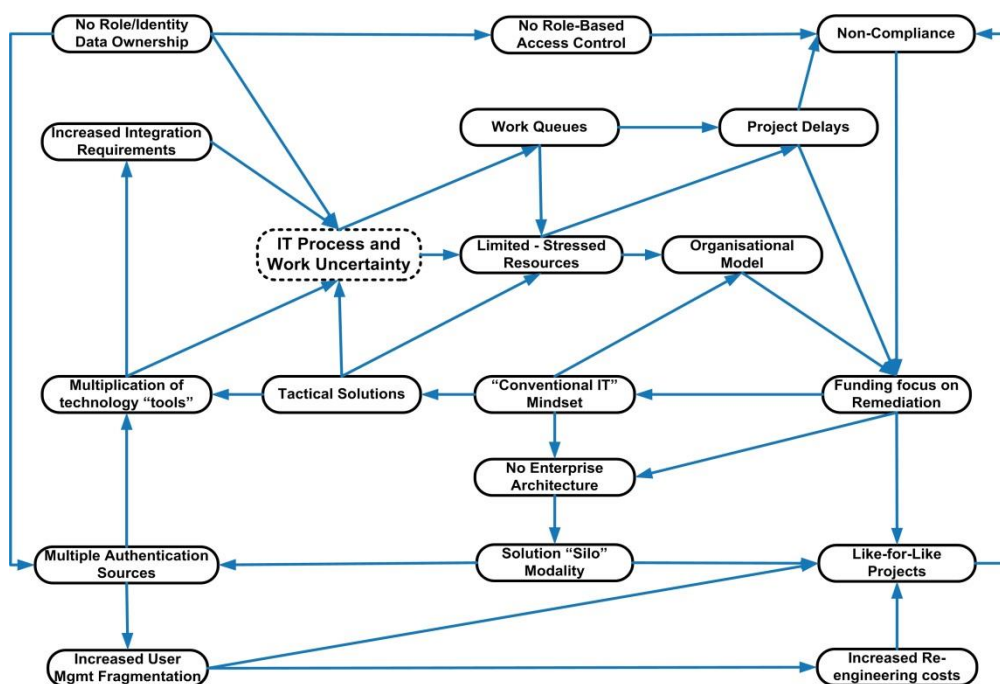
Contrary to this, we see a troubling scenario in most organisations of all sizes: organisational Security is severely misunderstood, and has become only a box-ticking exercise in compliance. Even worse, both in the industry and the consultancy sector, there is still a widespread belief that Security can somehow “exist” without Identity management. Many practitioners also like to say that it is “difficult” to sell Identity management to the business teams. Thanks to my experience in many organisations and sectors I am witness to a long catalogue of excuses and evasive responses when it comes to the Duty of Care, both in Security teams, organisational leadership and external advisors and technology suppliers. Here is a sample of the excuses the reader may have heard from teams and people refusing to adopt Identity data ownership and controls:

- “Centralised user management is not in our policies”
- “Cost avoidance is not relevant as it does not represent real expenses”
- “Our supplier would not transfer costs savings to us”
- “Identity data is not included in my area”
- “I need to reduce the risks of my project”
- “It is not part of the Business or the Information Architecture”
- “It is too expensive”
- “It is too complex”
- “It needs new business roles which we don’t have”
- “It needs too much effort”
- “It needs too much time to fulfil”
- “It would benefit the service providers but not us”
- “Our focus is now on integration, not on transformation”
- “Somebody else did it and failed”
- “Our funding model does not support cross-divisional projects”
- “There is no urgency to do it”
- “We are already doing manual access remediation”
- “We don’t have the necessary experience and skills”

Within a conventional approach, all these rationalisations could be “understandable” and “justified” perhaps as an expression of the limited scope of action of managers and team leaders, but in reality—especially if we consider all these expressions together—they reveal a disastrous state of mind and a

lack of governance and direction inside normal and respectable organisations. This is what I call “dereliction of the duty of care,” even when I am conscious that in the current management scenarios, managers are not supposed to go beyond what they are asked to achieve. Any holistic view of the perennial problems of Identity and Security would be “outside of their remit.”

For sure in the past few years, many organisations have tried to disentangle themselves of this situation, but a lack of understanding of the roots of the problem doomed these efforts from the start. This is what I have covered in a previous chapter when considering the problems of “project failure.” In my view, the causes are deep. The dereliction of the duty of care in respect to Security and Identity management is not the result of some entrenched management practice but the precondition of IT practice. In fact, it is only by managing Identity data in an ad-hoc, expeditious way that we can build the current type of IT services and infrastructures. IT, especially in complex organisations, needs to ignore, postpone and fragment Identity management with the result the IT landscape itself is indelibly marked by this implicit rejection. So when organisations try to remedy their Identity practices by joining the IT infrastructures, we have a sign that they have got the wrong end of the cause and effect chain. I documented this maze of interactions showing how these factors interact.⁵ The diagram shows the direction and impact of various organisational problems in Security and Identity management.



organisational and business excellence before we address any technological matters. The disciplines of Trust Definition and Allocation are closely associated with the aspirations of the business leader and his or her “take” on the market. If we do not believe in this and instead present a spurious “risk” and “cost-benefit” discourse devoid of any strategic purpose then we should not be surprised by failure.

Information Insecurity

Given the complete focus of current Security disciplines on “data protection” and information as an “object under threat,” it is only fair to evaluate how we are doing in the “cyber-war.” We saw in earlier chapters that project and programme delivery were a dark area, devoid of encouraging results. Perhaps we do have some positive news in the more specific subject of “data protection”? Sadly that is not the case. Before continuing, to eliminate any ambiguity, I want to reassert that Security and Identity management, in their objective side, include controls over data “at rest,” “in transit” and “in process,” but the emphasis is not on data as an object or a mechanical flow, but on data as interaction and multilateral process. I like to use the term “quantitative identity management” in the sense that informational exchanges can be measured by taking read and write operations as the tokens of real organisational processes. In this way, data becomes a reflection of organisational functions.⁶

Now, either in this perspective –or in the conventional one-- “data” can still be described as something material (“tangible”) that is moved around in the organisation. This image is easy to understand when speaking about “data loss” and “data breaches” as a manifestation of the failures of conventional information Security solutions. The practitioner is standing on a space composed by one or more “enterprise” data infrastructures (databases, file servers, portals, applications), which contain “informational assets” and are under constant and diverse “attacks.” The usual dangers come from a series of insecure practices or technical defects that put data “at risk.” The most important of these problems can be catalogued as follows:

- Denial of service. Under stress or attack, computer systems expose their limits and coding errors. Expert attackers or any determined person can destroy or access information when systems misbehave and fail. A very frequent form of attack is the so-called Denial of Service. More or less large sets of compromised computers can be turned on to attack organisational infrastructure, leading to service loss and in some cases to data corruption.
- Excessive access rights. It is a usual scenario in all types of organisations, where users and their tools (the programs they use to work) have access rights that do not correspond to their business functions, being “higher” or “wider” than they should be. This problem, also called “excessive privileges,” allows users and information processes to read or write from and to confidential data repositories. As users come and go from organisations, or move from one role to another, they accumulate access rights to systems and services beyond their “need to know.”
- Privilege elevation. Privilege elevation is a normal procedure in systems management, by which an operator, using available tools, changes the level of access to be able to carry out some tasks that require more authorisation. The problem is that unauthorised persons (inside or outside the organisation) can also raise their access scope if they know the process. In some cases software limits and errors help these actions; in other cases the systems themselves have facilities to do so.

- Abuse of access rights. Even when users have properly assigned access rights, these can be utilised for illicit or destructive purposes. It has been clear for years that a large proportion of data breaches and loss occur within the organisation itself through this abuse. This danger is higher and more complex the higher the person is in the organisation, and the more access rights he or she has overall.

Confronted with these dangers and attack types, how do organisations fare? It is not possible to find complete documentation about this, because organisations do not share the actual state of data controls. A growing debate exists about the need to legislate data breach disclosure, but I won't discuss that issue here. There are nevertheless limited scope studies which point us in the right direction, for example the work by Dana Rosenfeld, Alysa Zeltzer and Christopher Loeffler⁷ cataloguing the gaps in organisational information Security. While their study is focused on Personal Identifiable Information (PII) their findings can be generalised to all types of data. In my own practice I have found that also business data is affected by problems that we can list as follows:

Common Gaps in Information Security:

- Not developing policies in the first place or failing to implement policies.
- Not designating specific employees or groups of employees to maintain and implement the program.
- Permitting the haphazard collection and sharing of information inconsistent with policy requirements.
- Not updating or modifying policies as the business's information practices or laws change.

Common Gaps in Information Storage and Disposal:

- Not knowing what information is stored by the company and its location.
- Security levels that are inconsistent with type of data stored.
- This may include the failure to encrypt and/or truncate sensitive information as required by applicable law or as recommended under industry guidelines.
- Not limiting access to information to those having a "need to know" that information to perform their duties.
- Retention of information longer than necessary to carry out the original business purpose.
- Improper disposal of information that is no longer needed.

I am sure that all Security experts and practitioners have seen the typical scenario where the organisation in fact does not know and does not have means to know what information is stored in their file servers and who has access to that information. On the other hand, we also have seen many times heroic efforts by business managers and Security-concerned team leaders to establish some form of control over information repositories, only to find in the end that "nobody" owns the data and hence there is also nobody to sign off any security policy over it. Judging from experience, the "gaps" listed by Rosenfeldt and Zeltzer are effectively the norm, the "state of the matter" in organisational life.

So, how can there be “system” Security--either in the old or the new definition of the term-- if we have such gaps in governance and control? To expand this further, we could also ask: how can there be Identity management if even *business data* management (usually including personal identifiable information or PII) is in disarray? To be clear, organisations, especially in the financial sector do have the functions of “data ownership” and “data governance,” but in too many cases this is limited to large customer data stores and does not include staff, partner, supplier, contractor or any other external collaborators.

In spite of multi-year Identity programmes, many organisations do not have the same criteria for customer and staff or collaborator identity data. To progress from where we are, my suggestion is that Security and Identity management should learn from existing business practices centred on Data Integration and Warehousing, and apply their more advanced rules and practices. Data Management experts may smile at reading this, surely knowing that their own area leaves many things to be desired, but I can confidently say that they are years ahead of the Security professions. A System cannot be secure without data governance, specifically without Identity data ownership and management. This is a difficult task, but appropriate models exist and there is no need to invent anything new.

Data Governance is always a continuing programme--not a “project”--which must be planned and led at the highest levels of an enterprise. It will not happen without personal commitment for excellence from the owners of the organisation *and* the representatives of the owners. This is not an optional process and it has to be asserted within the business model itself. Without this it will always be difficult or impossible to allocate resources and enforce organisational policies. It should also be clear that Data Governance in general and Identity governance in particular are not functions of the IT department. As heroic as it may seem for some IT leads to declare that Identity is their responsibility, obviously governance has to involve accountability and sign-off capacities which do not exist within the IT departments.

All the terms and practices that are part of an organisational Information Architecture are also part of a Security and Identity data management strategy:

- Data Access
- Data Architecture
- Data Archiving
- Data Cleansing
- Data Compliance
- Data Governance
- Data Migration
- Data Modelling
- Data Monitoring
- Data Ownership
- Data Policies
- Data Privacy
- Data Profiling

- Data Quality
- Data Retention
- Data Retirement
- Data Security
- Data Standards
- Data Stewardship
- Data Storage
- Data Structure
- Data Taxonomy
- Data Traceability
- Master Data Management
- Metadata Management
- Reference Data Management

Also in this respect, as I mentioned above, nothing needs to be invented, and we, the Security practitioners, should instead turn to the more or less standard manuals of Data Integration and Information Architecture which have been available for decades now.⁸ Essentially, the aim of data integration and governance is to provide accurate, reliable data (a “single version of the truth”) across the organisation and outside of it, to partners and external interested parties, including consumers. To do this, much more than technology is necessary. First, the organisation needs a common language and common standards for data classification and management, and –more critically–special roles and responsibilities have to be defined and assigned: the data owners, custodian and stewards.

In most cases—especially for Identity data management—a global team will be necessary, to work out the standards and execute the governance processes across many different countries and technologies. Against these needs stand many obstacles of an organisational and “political” nature, for example differences in “how business is done” in each division or who is in charge of data depending on the country or the sector. Therefore, this is *even less* a technological task than can be imagined at first sight and cannot be accomplished by the IT departments. In fact, it is essential to understand that in terms of Systems security and organisational transformation the IT department has a decreasing role as we progress to wider and more complex networks of cooperation. They can be “custodians” and implementers of the processes needed, but they do not lead or own these.

The current Situation

While the change is still evolving and organisations open their eyes to new possibilities, data insecurity and loss are present. Some statistics will show how ineffective Security controls are in today’s organisations. A 2006 survey among 100 IT Security professionals, conducted by Computer Economics,⁹ shows a list of Security threats, out of which I highlight the following:

- Insider threats are the highest-ranking IT security concern, specifically insider misuse and unauthorized access. The greatest “risk” to the organisation resides with those inside the security perimeter.

- Unauthorized access by “outsiders” figures second or third among the Security concerns, but the report highlights many organisations do not know who may have gained unauthorised access.
- It is a well-known fact that “hacking” incidents are underreported in the statistics.

A PricewaterhouseCoopers survey from 2012¹⁰ complements these insights, showing that while many companies appear to understand the new dangers coming from an expanded user network, little is done to “secure” information in the changed circumstances. For example, the survey notes that “many companies are not doing enough, and some are not doing anything at all, to secure their mobile environment.” The report shows concern that too many organisations are not taking threats seriously. Simultaneously, 82% of large organisations are mentioned as having reported security breaches caused by staff, including 47% who lost or leaked confidential information.

Given the lack of policies and the gaps listed above, it is not strange that data breaches are a permanent feature in the business and IT landscape. On January 2011, for example, the Identity Theft Resource Center (ITRC), based in the United States, published statistics¹¹ of the reported US data loss incidents in 2010 listing 662 reported events, nearly a 33% increase over 2009. Given the way the data is reported and collected, observers think the number of data breaches is higher. The ITRC itself highlighted in the report an obvious lack of transparency from organisations: “Other than breaches reported by the media and a few progressive state websites, there is little or no information available on many data breach events.” Data losses consist mostly of personal information, like social security numbers (62%), and Credit Card details (26%).

The ITRC report points out that 51% of publicly reported data loss incidents also disclose the number of records compromised or destroyed, coming in at a total of 16.1 million records. That means that about half of all the reported data breaches do not reveal the number of compromised or lost records. It is interesting to note the reported incidents were 498 in 2009, 657 in 2008, and 446 in 2007.

Among the incoming information about data losses and Security failures, though, some functionaries do not see a cause for alarm, even if the numbers are staggering. For example in September 2012 the UK Deputy Information Commissioner David Smith¹² told Computing magazine that “while he does not dispute the accuracy of figures to suggest a 1,000 per cent rise in UK public and private sector data breaches in the past five years, he is unsure they “reflect the position” of serious data leaks.” He may be right indeed, because it is not possible to know what was lost or if the reported data losses are all that took place. From my point of view this does reflect two things though: the increase of reporting due to regulatory pressure (especially in Europe) and also a continuous expansion of the problem. In any case, even if this does not reflect the gravity of the situation in every sense, what the reader should retain is that, whatever measures Security professionals have been proposing, either these are not working or else they are not being adopted.

At the current rate, many successive years could be named “The Year of the Hack.” In fact, it can be asserted that every organisation, including military and political entities, are suffering because of this. High-tech companies are not the exception. In January 2012, another report by the Identity Theft Resource Center identified hacking, followed by data lost in transit and insider attacks, as the leading data breach causes in 2012.¹³ This report follows the data collected for 2011 for disclosed data breaches (a total of 419 events). That year, “[...] targeted intrusion into a data network,” including card-skimming attacks--were at an all-time high, and responsible for 26% of all known incidents. The second cause of breaches was the loss of data on the move (18%) consisting of data stored in mobile devices or printed for transportation. The third cause was classified as insider theft (13%). Overall, the ITRC indicates that malicious attacks--including insider and hack attacks-- represented 40% of the disclosed data breaches in the US, while 20% of breaches were the result of “accidents.” In 2011, 22.9 million records were compromised, of which 81% included social security numbers.

The ITRC makes a point when stating that in 2011, the US government and armed services saw the greatest volume of compromised records (comprising 44% of all exposed records), followed by non-financial businesses (33%), medical and healthcare groups (16%), educational institutions (4%), and banking, credit and financial firms (3%). The report says: “Non-financial businesses, as well as medical and healthcare groups, saw the largest incidence of insider theft, while non-financial businesses were hacked far more often than other industries. Notably, 17% of all breaches involved hack attacks against businesses, compared with hack attacks against banking, credit and finance (3%), education (2%), medical and healthcare (2%), and government and military (1%).”

The report is also frank in stating that in the year 2011 only 52% of publicly disclosed breaches detailed the number of sensitive records that had been exposed. This alone means that it is impossible to estimate the damage caused to companies and individuals, or to certify the distribution of attacks and losses. It nevertheless gives us a picture of the problem. What are we as Security experts and professionals doing about it? Is it comforting enough to continue with the rationale that “the business” or “the managers” don’t get Security or Technology?

Here are also some statistics about the cost of data losses, to match the information given above. One such case is exemplary.¹⁴ The reference quotes the Global Payments SEC 10-K/A filing of the same date, containing estimates of the 2011 data breach incident. The text says: “For the year ended May 31, 2012, we have recorded \$84.4 million of expense associated with this incident. Of this amount, \$19.0 million represents the costs we have incurred through May 31, 2012 for legal fees, fees of consultants and other professional advisors engaged to conduct the investigation and various other costs associated with the investigation and remediation. An added \$67.4 million represents an accrual of our estimate of fraud losses, fines and other charges that will be imposed upon us by the card networks. We have also recorded \$2.0 million of insurance recoveries based on claims submitted to date as discussed below.” And it adds: “We expect to incur additional costs associated with investigation, remediation and demonstrating PCI DSS compliance and for the credit monitoring and identity protection insurance we are providing to potentially-affected individuals. We will expense such

costs as they are incurred in accordance with our accounting policies for such costs. We currently anticipate that such additional costs may be \$55 to \$65 million in fiscal 2013. We anticipate that we may receive additional insurance recoveries of up to \$28 million.” The cost per lost record has been variously estimated between US\$100 and \$190.

All types of organisations are suffering data losses, including those that set the standards. In September 2012, the public learned the Institute for Electrical and Electronic Engineers (IEEE) had lost 100,000 user names and passwords by exposing them in an open server on the network.¹⁵ This was painful for an organisation dedicated to technology standards development, continuously working with major global and national organisations. The exposed files had been stored in an unencrypted form and in a plainly accessible folder. For sure the Institute closed the gap soon and asked the users to change passwords immediately, but it was also the occasion to remind everybody that data security – even using the conventional approach—cannot be protected if it is not classified, and it won’t be classified if it is not governed like an asset. When people think of “proactive” measures and leave for a moment the techno-centric approach, they should have in mind higher orders of leadership and purpose.

What Security is not

The lack of Direction and Trust management leads to several wrong conceptions that are obstacles for an integrated Security strategy:

- The belief that Identity management can be reduced to the so-called cyber-security trend. While it is clear that cyber-security (as it commonly understood) is relevant for some organisations, its essence is not Identity management. These areas share technologies but their goals are different: while the first addresses unknown attackers and articulates the notions of warfare, attack & response, counter-attack, etc., the second is founded on a generalised intention to allocate trust, facilitate access, decentralise controls and enable the end users to manage their authentication credentials.
- The belief that Identity management is centred on regulatory compliance or the “protection of informational assets.” This comes straight from the past of our Security disciplines: First there was “asset protection,” directly linked with over-centralised business processes and lack of autonomy of the users; then there was Governmental pressure to assert data regulations. The result was a combination of Protection of assets and Data protection measures, which is commonly taken as the essence of Identity management. This confuses the historical evolution of the disciplines with their ultimate goals.
- The predominance of provisioning technologies (account management) as the essence of Identity management. This trend is strongly maintained by large technology vendors and is the product of years of haphazard and chaotic growth of IT infrastructures. At some point organisations find themselves sunk in a confusing and anti-economical technology maze and try to overcome it by buying more technologies: “provisioning,” “user management,” “user recertification,” “risk-based reporting,” etc. When these solutions are rooted in the usual silo-orientated approach (which is the continuation of the style that produced the chaos in the first place) little can be achieved.

Combinations of these three wrong conceptions can be seen everywhere, and their effects are then translated into the catalogue of excuses that we saw before. The worst cases are those where a techno-centric solution is supported by compliance and protection drivers and tinted by “cyber-warfare” ideologies. It is difficult to see in this confusion where we are going. A closer analysis shows that behind all these misconceptions the key issue is that Identity data (especially staff, partner and collaborator Identity) is not managed as an asset. In the organisational plane, the lack of direction is revealed by the fact that there are no data owners and no governance process exists.

To understand what is happening here it is essential to turn to the history of the Computer revolution. This revolution, itself arising from a changed world society, essentially created the individual technology user, the connected, remote worker. Nevertheless, the techno-centric perspective leads people to “forget” these and propose actions and ideas that negate this origin. Where the PC puts power in the hands of the individual, some technologists insist on recovering and centralising computing power, ignoring the social history of computing. Where the Cloud is based on an expanding variety of users, some technology suppliers want to reduce this to a single “cloud user” type. The problem is that in doing so, the techno-centric mind disables itself for anything relevant in Security matters, multiplies the threats and gives bad and costly advice to the organisations it claims to serve.

Outside of the Perimeter

In a recent article in SC Magazine, Dan Raywood points to the critical change that is occurring in the Information Security market. He quotes Paul Simmonds, former CISO of AstraZeneca and board member of the Jericho Forum, as saying: "The issue is on the move outside the perimeter, which is driven 100 per cent by business and the IT administrator is playing catch up, as is security."¹⁶

Simmonds suggests the main challenge with Identity Management is the difficulty if not impossibility of containing the identities within the perimeter as business drivers lead to a fragmentation of access routes and business channels. To counter this, Simmonds recommends the separation of access management and identity management via the use of "claims-based security." Claims-based mechanisms¹⁷ are relevant but, to begin with, it is important to focus on the two things that are being highlighted here and will be even more important in the immediate future: first, the perimeter is disappearing, or has disappeared altogether in large global organisations; and second, Identities are fragmented and access routes (even for company staff) are multiplying and changing in nature.

In essence, Identity fragmentation and diversification compounds the well-researched problem known as "deperimetrisation" of IT environments.¹⁸ To address this it is essential to re-balance and re-focus Security moving from the emphasis on Protection and Enforcement to Trust Definition and Trust Allocation. In terms of Risk it is essential to adopt perspectives geared towards Risk-Taking and Risk Sharing as I have explained in other chapters in this book.

Contrary to the necessary readjustment, too many documents and statements coming from the Security experts repeat the language of risk avoidance and the criteria of “risk appetite,” as if we were

permanently talking only to IT departments. As Simmonds says, IT departments are only “catching up.” In this context, it is a losing game to continue patching and upgrading “the system” as the future does not look good for such a stance. A risk avoidance position does not carry the voice of the business leader or the risk-taker. It can sustain only a minimalistic investment curve, meaning that it will support an expedient solution to “get away” with the necessary controls, to “manage” the consequences of internal and external audit processes, not aiming at expanding the business, growing the market or increasing the variety of users.

When Security practitioners accept these limits, they follow the fears and misunderstandings that persist in the IT professions. Why use the notions of “counter-attack” and “rapid response” as if all of Security depended on warfare scenarios, external penetration and “inbound” threats? Why is Security not thought of as a business enablement force? It is urgent to reiterate that on the ground of conventional security, experts and practitioners become followers and not leaders.

¹ E.L.Trist, “The evolution of socio-technical systems: A conceptual framework and an action research program,” 1981

² Günter Ropohl, “Allgemeine Technologie : eine Systemtheorie der Technik,” Universität Karlsruhe, 2009

³ The Octave web site: <http://www.cert.org/octave/>

⁴ E. Granstedt, T. Nolan, “Paradigm shift necessary to address advanced persistent threats,” 2010, http://www.gsnmagazine.com/article/20675/paradigm_shift_necessary_address_advanced_persiste

⁵ Carlos Trigoso, “Negative Feedback Chain in Solution Definition and Execution,” 2008 - <http://carlos-trigoso.com/public/praxiology/>

⁶ See chapter 7: Quantitative Identity Management.

⁷ D. B. Rosenfeld, A.Zeltzer and C. M. Loeffler, “Common Gaps in Information Security Compliance Checklist” , Kelley Drye & Warren LLP - Practical Law Company 2011
http://www.kelleydrye.com/publications/articles/1551/_res/id=Files/index=0/Common%20Gaps%20in%20Information%20Security%20Compliance%20Checklist_Feb2012.pdf

⁸ An excellent reference is the “Information Service Patterns” series by Dr. Guenter Sauter and his collaborators at IBM, <http://www.ibm.com/developerworks/webservices/library/ws-soa-infoserv1/>

⁹ Computer Economics Magazine, “Trends in IT Security Threats” 2007

<http://www.computereconomics.com/article.cfm?id=1214>

¹⁰ Information Security Breaches Survey <http://www.infosecurity-magazine.com/view/25232/pwc-2012-information-security-breaches-survey-preliminary-findings-report-continued-mobile-insecurity/>

¹¹ See: http://www.idtheftcenter.org/artman2/publish/m_press/index.shtml

¹² Peter Gothard, “Deputy ICO says big rise in reported breaches is no cause for alarm,” September 2012 - <http://www.computing.co.uk/ctg/news/2207131/deputy-ico-says-big-rise-in-reported-breaches-is-no-cause-for-alarm>

¹³ As reported by Mathew J. Schwartz, InformationWeek, January 12, 2012
<http://www.informationweek.com/security/attacks/hack-attacks-now-leading-cause-of-data-b/232400252>

¹⁴ <http://www.databreaches.net/?p=25453> September 28, 2012

¹⁵ InfoSecurity Magazine, “IEEE data breach offers up 100K member logins” - <http://www.infosecurity-magazine.com/view/28465/ieee-data-breach-offers-up-100k-member-logins/> and <http://www.databreaches.net/?p=25400>

¹⁶ Dan Raywood, “Jericho Forum: Identity and access management need to be separated in the business,” 2011- <http://www.scmagazineuk.com/jericho-forum-identity-and-access-management-need-to-be-separated-in-the-business/article/199154/>

¹⁷ See: Keith Brown, “Exploring Claims-Based Identity,” 2007 - <http://msdn.microsoft.com/en-us/magazine/cc163366.aspx>

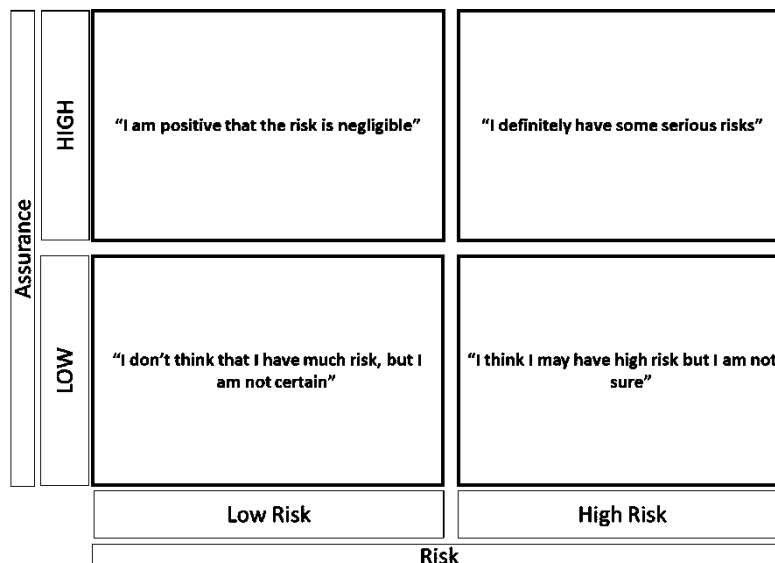
¹⁸ The Open Group Jericho Forum website: <https://collaboration.opengroup.org/jericho/>

9. Persistence of Techno-Centrism

The Fundamental Conceptions

In several places in this book I described the Four Security Perspectives, a model which guides my work in Security and Identity management. The fact there are four aspects may not be surprising for IT specialists, but it merits discussion from a philosophical perspective. Why are there four, and not two or six? When presenting these ideas to Management Consulting audiences and IT Managers in particular, after some smiles of complicity, nobody discusses the external aspect of the model even if people disagree with the details. After all, consultancies are always talking about “quadrants” and “dimensions.” The models may differ and the terminology is diverse, but we are familiar with this type of graphic classification, where we correlate some features against others.

Obviously, we take as a reference (sometimes unconsciously) the system of so-called Cartesian coordinates (x and y dimensions arranged on the geometrical plane), by which we can associate values on one dimension (e.g. “x”) against another (e.g. “y”). More ambitious models will add other dimensions: three, six or eight (for example in the “radar chart”).¹ What is noteworthy though is the underlying mechanism of such models. This is rarely discussed in technological milieus, but in fact every quadrant-based model and their variations are based on a “logic of distinctions.” So, for example, two dimensions will always determine four quadrants. The choice of dimensions used for the comparison is arbitrary, but obviously the consultant will try to make sense by choosing some close to the subject under discussion.



Assurance and Risk diagram - Arca Systems²

Let us retain in mind when we see a four-quadrant model, that in reality we are seeing a two-dimensional logic, even if the perception is there are four modalities determined by such a model. Philosophically speaking, there is no reason to stop at two dimensions, and we could even say that no number should be privileged in this sense.³ There is nothing necessary or transcendent about “four” that should limit us to four quadrants or their derivatives, but it is also clear that for normal communications and professional discourse, this number of logical distinctions is easy to handle and to explain. Some researchers think that the human cognitive apparatus has some limits regarding the number of distinctions that can be compared simultaneously and this may be at the root of the sense of “convenience.”⁴

A finer analysis tells us more about this class of “quadrant models.” While two dimensions always generate four quadrants it is also mathematically certain that each dimension (vector) must be graded itself, for the logic to function. The example shown before (comparing assurance to risk) in fact compares “low” and “high” risk with “low” and “high” assurance. In other words, on closer examination, we find that we are comparing two variables (for example risk and trust), but we are distinguishing two “states” within each of them. A more complex comparison is shown in the diagram below.

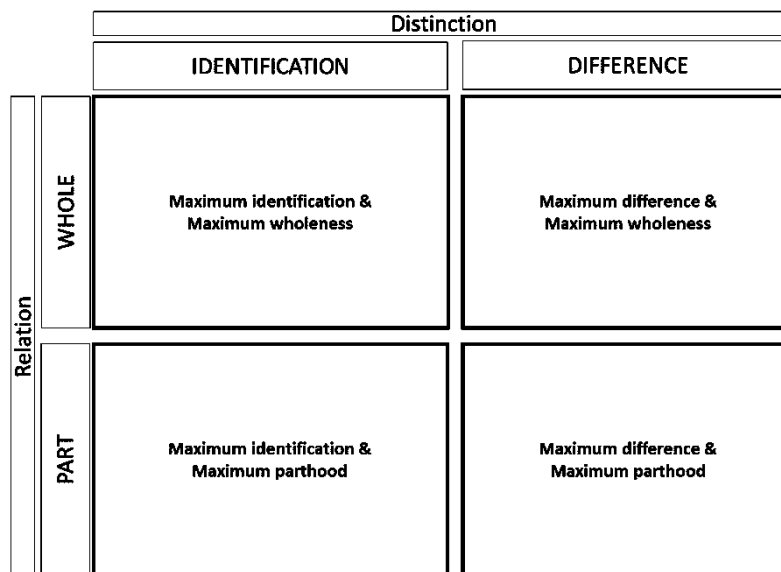
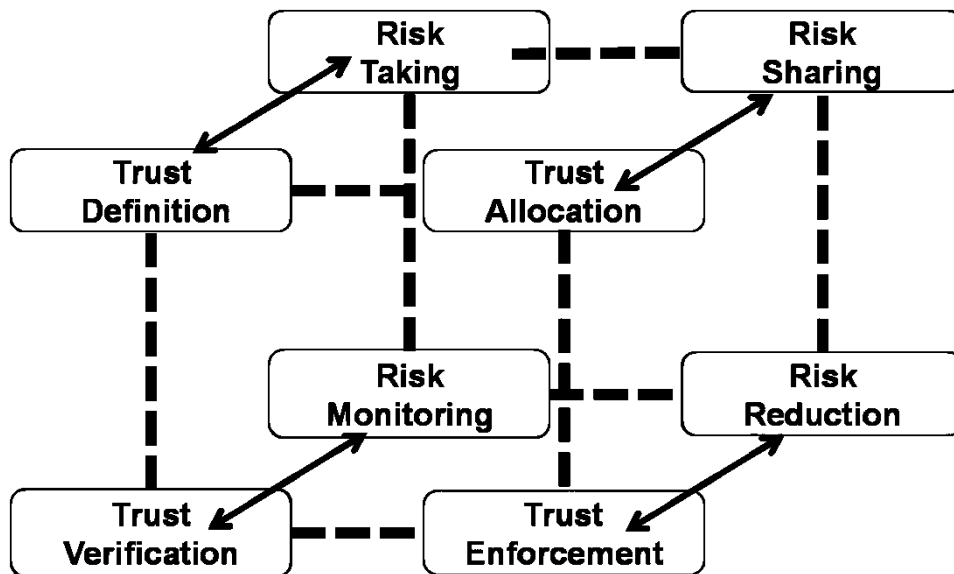


Diagram of Distinction and Relation⁵

It is worthwhile to say that this logic also works for continuous variables, i.e. for many distinguishable states for each of them. In this case though we see precisely that the number four occupies no special position in the logic even if it is a good “analytical” summary of what is happening. For example, an added level of distinctions for each variable will give not four quadrants but 16. It is difficult to see how effective this would be in our standard PowerPoint presentation in front of the proverbial 10-minute-attention-span executive.

So we settle for four quadrants, but are mindful that these are a summarisation and abstraction of a multitude of states and combinations that are logically possible. This is the point I want to stress here, so that the rest of this chapter is better understood. As the reader will see, in discussing the Security Perspectives, I developed a fourfold model, nevertheless always understanding that the number four does not have any particular meaning, and especially that it is not a supernatural value.⁶ In fact, when all aspects are considered, the model is not limited to two dimensions, as the complete Security model has to reflect the correlations between risk and trust.⁷



Four Perspectives of Risk and Trust (© Carlos Trigo 2011-2012)

This is a good place to suggest though, following the work by Professor Stephen Palmquist,⁸ that while numbers are not privileged in a specific way, odd numbers, in particular 3 and 5, can be associated with “synthetic” models, while even numbers, like 2, 4 and 8 can be shown to be “analytic.”⁹ In fact, even numbers just show clearly in their geometrical structure the underlying distinction mechanism (dichotomic logic), while odd numbers and the figures they represent (triangles and “stars”) hide the underlying dichotomies and present an image of unity. For example, the logics of Georg W. Hegel¹⁰ and Charles S. Peirce¹¹ are synthetic in the sense that they propose a “mediation,” a third entity bridging the gap between the initial dichotomy (e.g. in Peirce “firstness” and “secondness”). In comparison with these, the logics of Immanuel Kant and Heidegger are “analytical” as they keep the dichotomic structure in view for example in Kant’s “four judgements”¹² and in Heidegger’s “Geviert.”¹³

Understanding how human cognition is based on distinctions is not new and in fact has been useful in various areas of research. Notable examples of these applications are Chris Lofting’s work on neuro-cognitive roots of logic¹⁴ and Anthony Judge’s discussion on conceptual polarities,¹⁵ but before these

authors we had also the work of Will McWhinney¹⁶ on organisational change and the “personal construct” hypothesis of the American psychologist George A. Kelly.¹⁷ Other relevant authors are listed in the extended bibliography at the end of this book.

As a general formulation of what is relevant here, the reader should therefore keep in mind the fourfold model, and the Security Perspectives in particular, constitutes a logical, cognitive model, whose roots are beyond the realm of Security or Information Technology itself. So its descriptive power and its relevance does not come from the classification of Security areas and sub-areas that is here suggested, but from the underlying logical framework that it generates.

Empirical Views in Business

While discussing technology choices and Security strategies in our business, we often agree that a “good” solution is one where all business points of view and “stakeholders” are considered adequately; one where every angle of “interest” and “reason” is represented. This is especially the case when we consider the points of view of the executive management levels making the “final decisions” about any projects or investment strategies. There is a consensus among management specialists there are four concerns that need to be satisfied:

- a) The view of the Chief Executive Officer: When it comes to this view, it is often assumed the CEOs consider technology mostly as an enabler for organisational change and strategic advance. It coincides with the CFO’s view in looking for the overall reduction of production and operational costs, but the main concern seems to be the growth of the business with an eye on “shareholder value.”¹⁸
- b) The view of the Chief Information Officer: It is often said that this view focuses on the delivery of technical change to the business, while keeping the capital and operational costs under control. It is assumed that this view cares for the benefits gained from efficiency and employee productivity, within the expectations set by business strategies.
- c) The view of the Programme Managers: It is assumed that this view focuses on the minimisation of technical risks, and the delivery of technical solutions within assigned times and resources. Therefore, the Programme (and project) managers will think about the fitness of the solution and the compliance with established standards.
- d) The view of the Chief Financial Officer: This view seems to be centred on “rational” and managed control of investment and expenses, on extracting value of previous investment. The CFO puts much less emphasis on the technologies employed, and more on process control and confirmation. This –people think– is also the view that underlines strategic alliances with partners and suppliers to optimise the “value chain.”

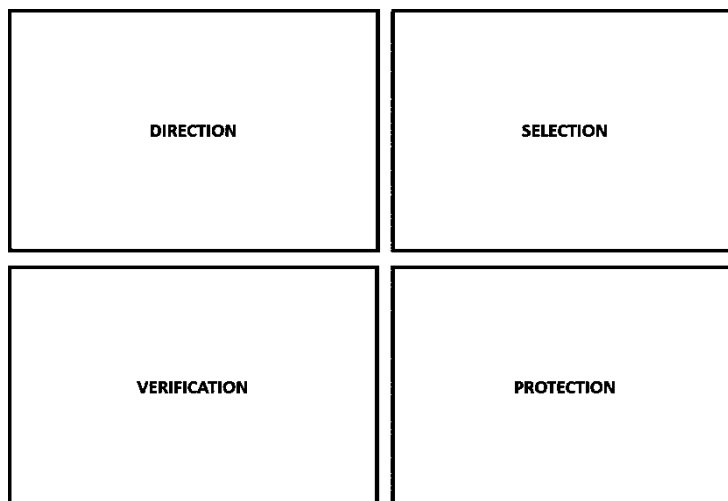
While these seemingly standard descriptions of typical “points of view” in the business are articulated around technology, we should not think that these are fundamentally about IT or related areas. In fact, many of the difficulties IT managers and departments have in their work in the enterprise stem from C-level executives addressing matters of technology from their own concerns and unilateral views.¹⁹

The four concerns roughly map to four logical positions that are visible in any IT or Security programme:

- a) The perspective of Direction, linked to strategy and leadership of the business as a whole, subordinating everything else to shareholder value and profit-making
- b) The perspective of Selection, focused on gaining benefits drawn from increased productivity and account management
- c) The perspective of Protection, centred on the effectiveness of the technical solution
- d) The perspective of Verification, focused on ensuring the auditability and validation of the processes and operations

It may seem arbitrary to “align” the C-level executive perspectives (even if we find this consistently in our experience) with the four orientations. On closer analysis though, these eight categories or classes can in fact be associated clearly. Let us return for a moment to the point I made in the previous section, to remark the essence of the matter is not the exact catalogue of issues and events that can be classified under each perspective. It is obvious there will be overlap across the C-Level stances; for example, if the CEO does have strong knowledge and opinions about financial strategies, it will not be difficult to see his concerns overlapping with those of the CFO. Often the CEO also has direct influence over the CIO operational space. What matters is the division of labour between the C-level roles and that this division of labour is not arbitrary but the product of organisational evolution and differentiation.

So what I am saying here is the C-level categories in fact are expressions of a deeper, more generic logical model of action, whereby organisational actors correlate to others within a model. For example, the CEO correlates to the CIO as the discourse of Direction correlates to the discourse of Selection, i.e. as the upper-left quadrant is related to the upper-right quadrant in the Four Perspectives model.



The basic diagram of the Four Perspectives © Carlos Trigo 2006-2012

It would not be excessive to underline again that a fourfold or “quadrant” model is a compression and abstraction of a multi-faceted reality comprising many more variables and distinctions, so the “quaternity” appears only as a logical summary of a very complex underlying reality.

When considering the Four Perspectives of IT and Security management, it is useful to think how these frame our solution and project work. We often find, for example, that an organisation’s project needs are primarily related to Sarbanes-Oxley²⁰ compliance, and therefore to the Verification disciplines. This regulatory compliance needs the certification of business documents (accounting and audit documents), by certifying –among other aspects—which user accounts are enabled on each of the “information and communication systems,” which individuals are associated with these accounts, who approved those accounts, and what is the status of the accounts and the users (active, inactive, suspended, terminated, etc.). In the present climate of increased regulatory pressure, especially since the Enron scandal in the USA, these are fundamental obligations that affect all the participants and “points of view” in the organisation.

At the same time, each of the participants and their teams will interpret the compliance requirements in a specific way, derived from their logical positions in the organisation, highlighting different aspects of the IT and Security management processes and systems. The IT Department and the teams under the Programme managers (the implementers) will focus on the access control aspects of the systems (the Protection aspects). The upper management teams around the CIO will focus on the account “life-cycle” aspects, for example on role-based controls and account approval processes (the Selection disciplines). On the side of the CFO and related functions, we will see instead an emphasis on audit efforts, account recertification and report production for external authorities. Finally, on the side of the CEO and related officials, there will be an emphasis on regulatory compliance as subordinate to the overall strategy of the organisation. This description comes from my practical experience, especially in the Financial Sector, but I am sure that it matches what Security professionals find everywhere.

These differences in emphasis and detail are somewhat compensated by overlaps and coincidences. When the discrepancies are deep –for whatever reason-- the organisation will have difficulty in executing its plans, and IT and Security management projects will be ineffective, compliance will be lacking and failures will be frequent. It is important to remark here that an organisation can be compliant even without technology, but technology cannot be successful without the convergent, coherent interplay of all the areas in the business. So, in the short term, the misalignment of the IT and Security perspectives is not a serious problem for the CEO, the CIO and the CFO if and when Sarbanes-Oxley obligations and other conditions can be addressed with or without the IT programmes and teams. I have to remark on this because my position is not that the private or public organisation “must” use technology for these purposes.

IT and Business Conflicts

The oppositions and correlations between the Four Perspectives are mostly evident in the conflicts between “the business side” and the IT departments and experts. This, as put by Aki Iskandar in an article published in 2011, “is nothing personal... but it’s getting worse.”²¹ Iskandar describes the case

of many companies that write their software solutions, where the IT Department and the non-technical managers and senior executives do not get along and are in permanent conflict.

The author explains these conflicts as derived from the “business” and the “software” life-cycle, two processes that “are out of synch,” according to him. He says that these life-cycles were not misaligned a decade ago, but the situation is deteriorating. His definition of the business life-cycle is “the period of time during which a company undertakes activities around the development of a product or service offering,” while the software life-cycle would be “a period of time during which a company undertakes certain activities around the development of a software product.”

Iskandar seems to think that while in the 1980s and 1990s the business life-cycle was 7 years long and the software life-cycle was three years in duration, the situation has changed. In his account, since 2001 the duration of the business life-cycle is only 1.5 years, while the software development cycle is 2.5 years long. Iskandar remarks: “The problem is evident and getting worse. People on the business side are upset because they simply don't trust that IT can deliver the software on time.” On the IT side, Iskandar describes a parallel sentiment: “[...] the situation is equally dismal. ‘Those managers - they want everything yesterday! Worse, they want their software built inexpensively and quickly, and they want it to be perfect. And they change the requirements every day!’ retorts the IT project manager.”

While this account is limited to the software aspect of IT and only to companies that “produce” their own programs, experienced observers of the IT world will concur the conflict of opinions described by Iskandar is actually the general situation across all areas in our professions. On the other hand, the change the author describes is not only related to the shortening of the business cycle (while the software cycle almost remains the same), but to other factors to which he does not pay attention. He points out that global competition is hastening the pace of business, changing the time that business leaders are willing and able to wait for new products, as they need to adapt constantly to new challenges. What is not clear though is why the software production cycle has not “kept pace”—as Iskandar puts it—with the business cycle.

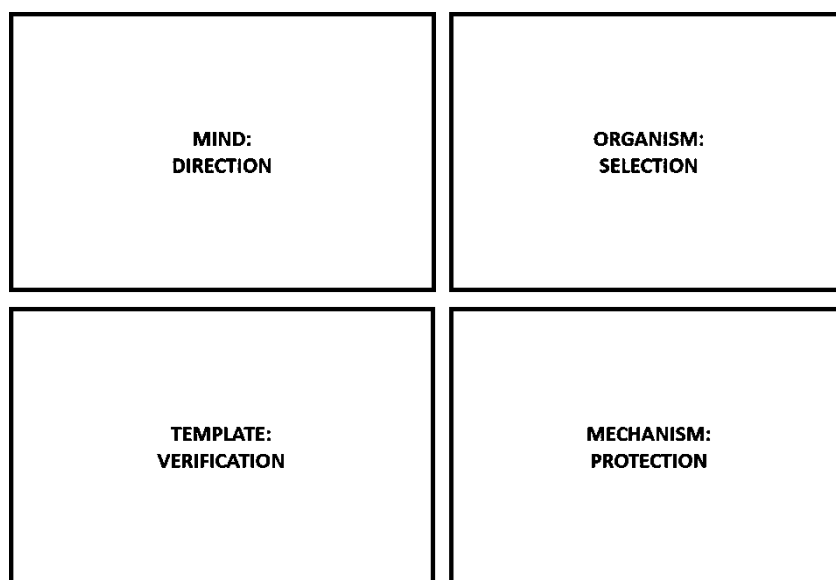
Let us leave now the constrained frame of companies writing their own software and look at the wider panorama. Instead of a choice of two or three languages for software development twenty to thirty years ago, we have now dozens of languages, and instead of one or two “platforms” to run those applications we have also many. Simultaneously, organisations find it increasingly beneficial not to write their own software and use “off the shelf” products instead. In fact, the widening and accelerating competition that is the main characteristic of this situation comes from organisations that do not follow the traditional “write your software” model. This change is parallel and supported by the trend of newer, faster organisations not to have an IT department at all.²² So the primary, relevant cause of the conflict is not the software development cycle being too long but the absence of need or reason on the side of the business teams for keeping an IT department and software development as part of the organisation. This trend is obviously accelerated if the IT teams are perceived as slow or ineffective.

In trying to address this conflict, it is essential not to see it as the product of two opposed camps (“the business” and “IT”) that do not understand each other or just have “different interests,” but instead as the inevitable fragmentation of the unity of organisations subjected to social and economic transformation. These pressures are external and internal to the organisation, leading to a wider range of opinions and choices, ending with a diminished role for the IT departments and its disappearance. Let us retain from this discussion the idea that conflicts are symptomatic of organizational change, and not the product of “misunderstandings.” Let us also keep present the idea that while in the past doing “your own” software and “your own” IT infrastructure seemed sensible, and nobody asked if business organisations had to have by definition an IT department and “technology” functions, today it is becoming evident that most technological functions are in reality external to the business models.

Four Root Metaphors

The techno-centric view, centred about IT infrastructure “availability” and Security “Protection” disciplines will always exist, although not as a part of the business organisations of the present and the future. This is what I mean by “persistence of techno-centrism,” and is one of the fundamental aspects of my philosophy. The persistence of the perspective is different from the need of IT as an internal organisational function.

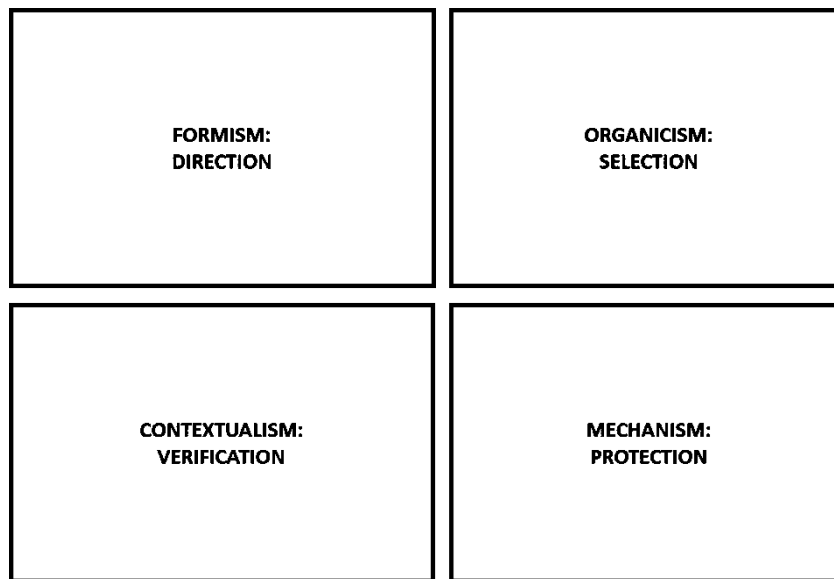
In this philosophy, the fundamental perspectives are as Richard Jung²³ would say, “mutually conceptually exclusive,” and we could add too that there are several relationships of contradiction and entailment between them.²⁴ Although opposed or contradictory, these metaphors depend on each other and are correlated so that each one cannot exist by itself. It is important to keep in mind that these are cognitive and logical modalities and do not need to be equally represented in an organisation. Their roots are much deeper than group or organisational structures and depend on principles that are common to all human activities.



Richard Jung's Four Metaphors and the Security Perspectives

In this sense, as a fundamental “hermeneutic metaphor” –in R. Jung’s terminology—techno-centrism will persist and cannot disappear as it forms an essential facet of human effort. To understand this it is useful to see the Four Perspectives also as manifestations of the World Hypotheses or Root Metaphors studied by the American philosopher Stephen C. Pepper.²⁵ Following Pepper’s model, we can immediately point to these Four Perspectives as world-views with deeply-rooted philosophical meanings. Here is how the Four Perspectives map to Pepper’s root metaphors:

- *Formism: Direction, i.e. definition of Trust, Risk-taking*
- *Organicism: Selection, i.e. allocation of Trust, Risk sharing*
- *Mechanism: Protection, i.e. enforcement of Trust, Risk avoidance*
- *Contextualism: Verification, i.e. verification of Trust, Risk monitoring*



S. C. Pepper’s Four Root Metaphors and the Security Perspectives

While the Mechanist metaphor stresses the disciplines of Protection against "objective" threats, the Contextualist paradigm underlines the disciplines of Verification and therefore the need for rules and processes. From its side, the Organicism will highlight the disciplines of Selection as the key to Security, and consequently the ideas of authorisation, delegation, membership and roles. Complementing the model proposed by John Arnold,²⁶ I introduced a fourth Perspective in Security, under the Formist metaphor. It should be called the discipline of Direction and remain focused on the ideas of definition of Trust Definition and Risk-Taking.

Arnold's "trust life-cycle" is a model of how an organisation gains trust in the objects it manages. The model says that an organisation needs some level of trust in every object, and that trust must be established, protected and maintained. The three steps of trust establishment, protection and maintenance match the three security service types described by Arnold in the cited paper. In my view, the circle needs to be completed with the Definition of Trust. While the "establishment of trust" can be mapped to the identity management processes, the protection of trust is associated with traditional Security measures at the level of the infrastructure. Maintenance of trust is then logically associated with the processes and rules used to ensure the access rights that were allocated initially are effectively monitored.

The definition of Trust complements these three, and constitutes the "missing Discourse" in the whole of IT (as explained in Chapter 1). Where the Security professions in the past took for granted the validity and even the existence of a Direction perspective, under which they were expected to operate, this is now an area that demands attention and action. In the present social and economic context, it is not guaranteed at all that the representatives of the business--including the nominal owners of capital-- will necessarily or naturally discharge the duties of their social and organisational roles. I have in mind the Financial Crisis whose last phase started in 2008, and its consequences in the business and professional spheres. Precisely because ownership and leadership are not guaranteed, and indeed because these are often absent from business organisations, there is no reason to assume that the organisation has defined, open and documented Information Security strategy, and therefore a defined Trust model. Enquiring the reasons for the absence of a Master discourse (see chapter 1) does not lead to some form of "rejection" of its social role, but instead to a deeper understanding of its place in a capitalist society, of the loss of Direction and its effects.

The techno-centric perspective (Mechanism) takes for granted the existence and effectiveness of the Master discourse. In other words, Mechanism assumes logically and socially the Information Trust boundary in an organisation is a given. That is the root of the impotent and desperate position of the IT technologists forever condemned to act in what they perceive a vacuum of strategy, an unending "misunderstanding" of what IT is about.

I am aware that this fourfold model of Security Perspectives does not match neatly the present and conventional understanding about our profession. It is difficult to see how logic models underpin our actions, because day by day we are involved in these ideologies and world-views as fish are surrounded by water. Also, in our work we do not see clear distinctions between the tendencies that operate in every organisation, but degrees and combinations of these, and "overlaps" between the underlying metaphors. At the same time, even limited experience in the IT field shows there is an order of dominance among the Four Perspectives or discourses. For example, it is obvious the dominant paradigm in IT and Security management is the one focused on Protection (Mechanism). The second paradigm in order of strength is Verification (or Contextualism, in Pepper's model).

When we see the organisation as a whole, as an object of study, it becomes clear the different paradigms arise from deeper roots that are not related to individual preferences or personal

inclinations. They are collective phenomena present in every organisation, as Magoroh Maruyama showed in his decades-long research programme.²⁷ This differentiation and opposition structure is universal and it would be wrong to confuse it with interpersonal conflicts or accidental issues that appear in business and organisational life. How the competing paradigms influence information security investment is clear once we consider the higher relative weight given to Protection and Verification in Security projects. This counts at least as indirect evidence of their action in organisational processes.

At a more general level, though, the oppositional structure here considered has much wider implications. Indeed, the most common presence of the Root Metaphors occurs in person-to-person conversations and in group discussions. When making a statement (uttering a proposition) the individual presupposes an opposite statement that remains unspoken. When we say “A” we necessarily hold in the background the concept of “not A”--i.e. the negation of the spoken statement. Further, opposition is not limited to negation, but also to entailment (implication) and contradiction, as has been exhaustively shown by Alessio Moretti’s work²⁸ with other logicians and philosophers: Fabien Schang,²⁹ Régis Pellissier³⁰ and Hans Smessaert.³¹ Moretti has pointed to the fact that this logical structure may have an even deeper model fundamentally equivalent to Jean Piaget’s “logical capacities” square³² and Walter Helbig Gottschalk’s “theory of quaternality.”³³ In other words, a statement is inevitably and logically linked with its negation, its contradiction and its implications. The oppositions occur in the unconscious, in a “zone” of the mind that could be described as a “verbal unconscious” for lack of a better term. Although this is not orthodox Lacanian theory, I think the French psychoanalyst probably was pointing to such a relation when he said the unconscious is “structured like a language.”³⁴

Moretti and the N-Opposition theoretical circle (led by the researchers quoted above³⁵), start from the foundations of modal logic, in particular the so-called Square of Oppositions. This “square” representing negation, contradiction and entailment of logical statements, originated with Aristotle and took its definitive classical form with Apuleius. I won’t summarise here the vast research that exists on this subject, but it is important to know that the immense interest that this has in philosophy, logic, mathematics and other sciences cannot be exaggerated. The N-Opposition theory website has many references to researchers working on the implications of the Logic Square in their own areas.

For my own research it was decisive to be able to match Moretti’s insights into this matter with the medieval logic of St. Anselm of Canterbury,³⁶ brilliantly analysed by Sara Uckelman and Douglas Walton.³⁷ Anselm develops the logic of action, a modal logic articulated around the verb “to do” (“facere” in Latin).³⁸ As explained in particular by S. Uckelman, St. Anselm had a unique approach to modal logic which can be compared with advantage to modern modal logic of action. In this logic, there are four main modalities:

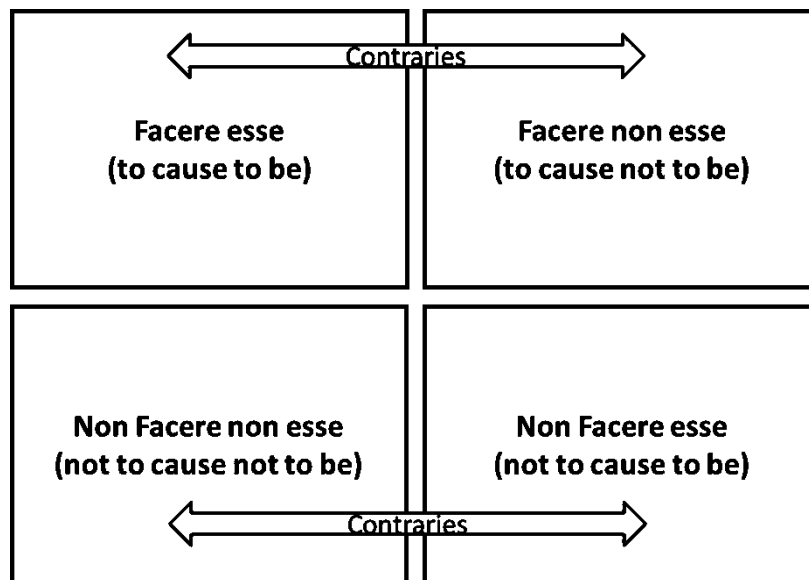
- **Facere esse (to cause to be)**
- **Facere non esse (to cause not to be)**
- **Non Facere esse (not to cause to be)**

- **Non Facere non esse (not to cause not to be)**

Using simple logical symbolism, these formulae may also be written as:

- **Fp**
- **F~p**
- **~Fp**
- **~F~p**

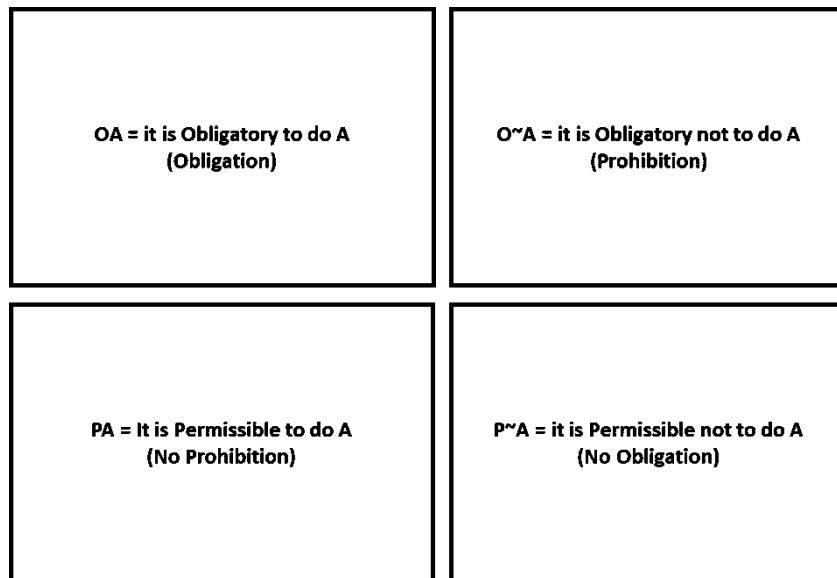
And a diagram may clarify the relationships between the logical terms:



Anselm of Canterbury's "Logic of Action" according to S. Uckelman

The studies by Sara Uckelman are in themselves interesting as they unfold a Medieval Logic which sheds a powerful light both on history and the nature of modal logic itself. Modern logic does not seem so "modern" after reading her analysis of Anselm's logic of action. For my own purposes, though, I find it particularly useful linking the logic of the verb "to do" –as proposed by Anselm hundreds of years ago---, with modern deontic logic, or the logic of obligation.

We can use modal logic symbols to depict a simple logic of obligation in the square of opposition as follows:



A simple deontic logic in the square of opposition

The reader probably will see that a logic of the verb “to do” maps neatly to a logic of obligation and permission, so “Facere esse” is compatible with Obligation (OA), and “Facere non esse” is compatible with Prohibition (O~A). The other two quadrants have similar equivalences. The most interesting point here is that through this translation, we can also reach a logical square that is immediately applicable to Security concerns, i.e. the concerns of reading and writing (as explained in previous chapters). A diagram shows this derivation:



A simplified logic of access control on the square of opposition

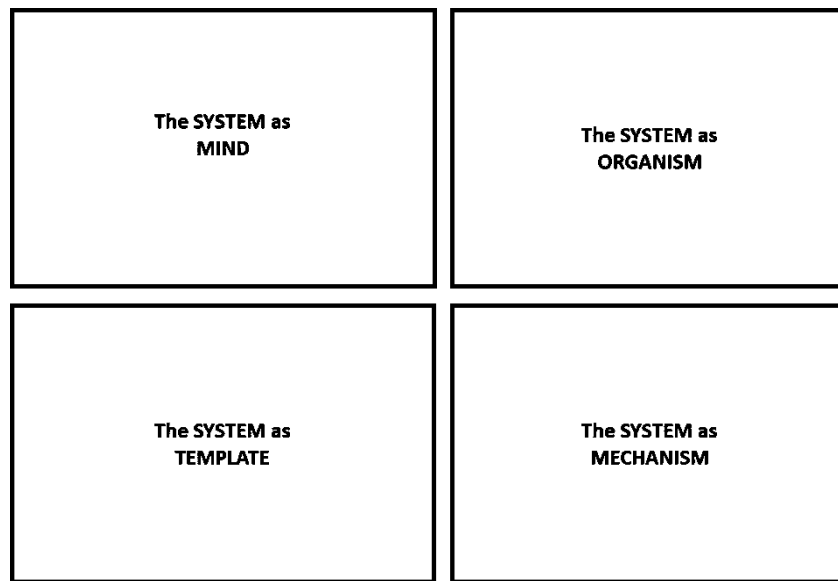
I suggest to the reader that this simple model contains the essence of the Four Perspectives in Security and Identity management. This can be seen from the fact the Obligation to give access can be only associated with the Definition of the Trust boundary of the organisation. Indeed, the business leader will set the context and limit of the population (market) he or she is addressing. Setting the trust boundary is a logical and economic operation that sets the frame for other complementary actions. Then, the Prohibition stance (“must not give access”) is evidently the allocation of trust; that is, the distinction of at least two groups (two memberships): those who have access and those who have no access. In sequence, the third stance, that of No-Obligation (which is diametrically opposed to the Obligation position), is associated with the notion of Trust enforcement, i.e. those actions by which access is given or taken (even to those in the group which has been allocated trust). Finally, the position of Permission (“may give access”) is the ex-post, contextual logic, where access may be recognised depending on evaluation of events.

These reflections do not exhaust the implications of oppositional logic for Security and Identity. My goal here is to explain that in addressing the structural constraints of human action (as manifested in logical modalities) we are throwing light on “alignments” and “conflicts” of opinion and practice that are pervasive in organisational life and professional work.

I want to close this section by briefly pointing to the fact that individuals act out these logical positions and move or “take turns” across the various perspectives, depending on their effective roles in the organization and each of the teams or levels they participate in. So people are not robots, but the communication systems they build in and outside of the organisation have their own laws and tendencies. People (the natural persons or individuals) are in the periphery of the organisations and only partially integrated into the “system.” We participate as “personas” (masks) or role players, but not as persons. In other words, persons are not sub-systems in the organization in any conceivable way; hence the oppositional logic of the organization, by which we see the Four Perspectives in action are not a choice of the individuals, but the contingent result of their interaction.

System Metaphors

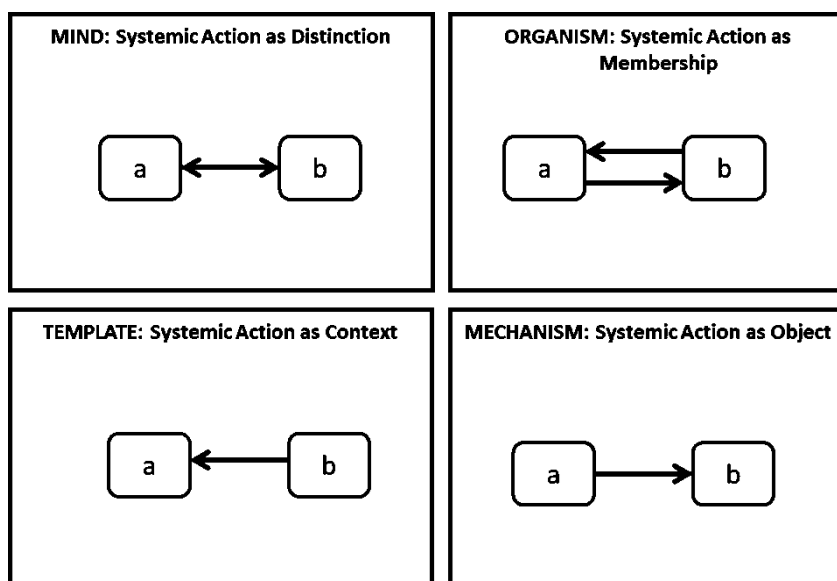
In this book I defend an idea of “system” that is not mechanistic. In fact, I think—following the work of Richard Jung and Stephen Pepper—there are four system metaphors which form an oppositional structure. Jung’s work on these matters brings philosophy into cybernetics. Not by accident, his main essay on this matter is titled “A Quaternion of Metaphors for the Hermeneutics of Life.” Again, the fourfold structure of this model should not distract us from the underlying logic of the proposal. For Jung, the core metaphors are those of Mind, Organism, Machine and Template.



Richard Jung's System Metaphors

I have translated this model to what I call “systemic action metaphors” which can then be represented by using the typical “boxes and arrows” diagrams of the technology-orientated professions. By boxes, I mean the objects that we are considering, while the arrows represent their relationships. It will become clear to the reader that I don’t think of these modalities of logic as isolated or standing each one by itself.

- **Systemic action as distinction (value function)**
- **Systemic action as membership (relationship function)**
- **Systemic action as object (material flow)**
- **Systemic action as context (process flow)**



The four metaphors of “systemic action” Following R. Jung’s Quaternion of Metaphors

This approach will serve to describe what I said in previous chapters about the fundamental conceptions of information. The key to this understanding is to start from the idea that information cannot be reduced to a unidirectional “flow of data,” and much less to an object. Only one metaphorical perspective or paradigm allows for such a reduction, which is the Mechanistic metaphor. Within this paradigm information is a material flow, and the “system” under consideration is a machine. Data “flows” from machine to machine in the world of the IT practitioner and this data flow can be conceived as “information.” In this sense we speak of a notion of “systemic action” where all activities in the system under consideration are conceived as “objects.” Within the mechanistic paradigm there is no action that is not an object.

Under a different systemic metaphor though, where the system corresponds to Jung’s metaphor of Mind, systemic action is a “distinction” (making distinctions or distinguishing what has value from what does not). Within this stance, information is an intangible entity, better described as “knowledge” about the world. Further, in thinking from the idea of systemic action as membership, borne by the Organism metaphor, information becomes a relationship, an association, instead of a distinction. And finally, in the lower left quadrant, where the Template metaphor is the key, information is a tangible process where the value is in the process, but information can equally be valuable or valueless. The following diagram summarises these relationships.

	ABSTRACT	CONCRETE
INTANGIBLE	INTANGIBLE-ABSTRACT • Information is knowledge • Meaning depends on purpose • Information has exchange value • Information is not material	INTANGIBLE-CONCRETE • Meaning depends on structure • Meanings change in the process • Information process has value • Information depends on exchanges
TANGIBLE	TANGIBLE-ABSTRACT • Information has no meaning • Meaning depends on context • Information is valuable after classification • Information is not material	TANGIBLE-CONCRETE • Information “is” meaning • More information = “more meaning” • Information (data) has intrinsic value • Information pre-exists exchanges

Modalities of tangible and intangible information (C. Trigos 2012)

Sociological Paradigms

My work on these matters owes a lot to Gurpreet Singh Dhillon.³⁹ Dhillon maintains that “[t]he management of negative events within organisations has become an issue commanding ever more attention from the various professions attending to the information needs of computer-using

organisations. However, the basic need for developing secure information systems has remained unfulfilled. This is because the focus has been on the means of delivery of information, i.e. the technology, rather than on the various contextual factors related to information processing[...] Although information system security is increasingly being considered as an organisational issue, the effort to prevent negative events has been aimed at protecting the technical infrastructure. This is largely because of the functionalist orientation of those responsible for managing information systems security. As a result the security professionals have been unable to address the social attributes of organisations."

In his approach, Dhillon largely uses the Morgan-Burrell model for sociological theory analysis, which consists of a fourfold classification: functionalism, interpretivism, radical humanism and structuralism.⁴⁰ Despite the criticisms addressed to this model, Dhillon adopts the "four paradigms as a means to classify the literature in information systems and to interpret the intellectual origins of the respective approaches." Dhillon concludes his study saying that "[w]ith respect to information systems researchers, there is a growing disillusionment with the narrow, one-dimensional viewpoint afforded by functionalist thinking. Although the importance of social issues related to computer-based information systems has been recognised, researchers are still locked into conventional thinking. In reality computer-based systems dynamically interact with the formal and informal environments in which they are used. Hence it is important to understand human interactions, patterns of behaviour and meanings associated with the actions of individuals. Even 'modern' functionalists have recognised the importance of such issues." And later adds: "By contrast to mainstream information systems work, the majority of the information systems researchers are still locked in a functionalist way of thinking. [...]The concern therefore has been on maintaining a security perimeter around information processing activities."⁴¹

Perhaps Dhillon's most important point, though, is this: "Security therefore is seen as means to protect something tangible and hard. However, occurring negative events, for which security is provided, cannot be viewed as discrete events. The prevention of such events therefore means more than just 'locks and keys.' It has to relate to social groupings and behaviour." In this way, Dhillon opens the way to a multi-paradigmatic view of IT and Security Management, as before him Hirshheim and Klein⁴² did with their analysis of Information Systems design. I claim to continue their lead in thinking that, when considering paradigms and metaphors both in organisational theory and information systems analysis, we should not stop at these aspects as given phenomena of organisational life, but as manifestations of deeper logical structure.

More specifically, we need to look at how Information is conceived and represented by each of the "root metaphors" or "paradigms." At the same time, in looking into the dominance of a model which relies on a concept of information as an object (a concrete-tangible entity) we must guard ourselves from the flat opposition or simple negation of that perspective. In the Morgan-Burrell model, this is the "functionalist" paradigm; in the Jung-Pepper model this corresponds to the "mechanism" metaphor. For example, aside of a polemical statement, it would be false to state that "Information has no value,

that it cannot be stored and that it does not flow." For sure, each of these assertions would be "true" within "organism" metaphor, for which not information, but the process of information transfer, is valuable.

Rhetorically we could still ask: If information has no value, why protect it? This would nevertheless be without meaning for the Organism metaphor itself, which is not centred on protection of informational assets, but on the idea of risk sharing and trust allocation (Selection). With good reasons we could say that information is not an object but an activity (informing or communicating), and we could affirm that information cannot be stored because it comes into existence only when it is read or used or interpreted. On the same lines, it is true that information only comes into being when there is a receiver, and therefore it is not clear if information "flows" from the source to the receiver or from the second to the first.

For actions and thoughts regulated by the mechanistic metaphor, information can be stored and can flow. The IT industry relies on this paradigmatic approach. All the IT technology is predicated on the storing and flowing of data! A simplistic negation of it would be at most polemical, but fruitless in the face of the deeper necessary roots of the four correlated metaphors.

The problem is not then that a mechanistic worldview exists. We know it exists and we know it is resilient and persistent. Its existence is not in question. The problem is that all IT disciplines are uncritically focused on Protection and only laterally pay attention to the other three perspectives. The Security market, including most products and service offerings, is focused on the "protection of informational assets."

It is far from established what information is, but within the Mechanistic paradigm we ignore these questions and settle for the common view that information "is" an object, that it has value and that it can be stored. Thinking within other paradigms can be unsettling or even impractical, because the Technologist and Security practitioner will not see the utility of such change. Despite this, I hope that opening new perspectives can help at least to see what we are doing and how we are doing it in a wider context. My goal is above all to show that we are dedicated to "information protection" not because this is the only possible way to look at information, but because we work within a specific world-view that dictates an ideology of information as an object.

If professionals were able to discuss what information is, and how to assess its value, without ideologies, we would arrive at surprising conclusions. Different parts of an organisation will have different measures and even definitions of information and the "value of information," trying to link the idea and the "being" of information to some Perspective or metaphor. In this process, for example, the levels of attributed value will be different according to the Perspective or Root Metaphor regulating the view.

David Sholle, writing about the dominant beliefs about Information Technology,⁴³ questions "[a]n economic philosophy that posits information as the source of value in a global economy; a business logic that focuses on the accumulation, production and management of data; media claims that

availability and access to information technologies represent an increase in choice and freedom; political projections that computer-mediated communication networks can solve the problems of democracy in the US; and a quasi-religious hope that technology can save us from our own excesses.” Sholle asks how is it that we have come to be so dominated by the idea of Information in the West. His answer goes to great lengths into a fundamental clarification of the problem but is limited when he arrives at the conclusion that “Information does not have a semantic context. Information has no meaning in the current context. The term information is applied metaphorically to processes that involve flow, storage, impulse. Information also conceived as a process, and knowledge as a stock.” With this evidently Sholle is working within the Mechanistic metaphor, searching for an answer, but unable to overcome one-sided beliefs.

I think though that Sholle’s approach, by linking Information theory and sociological thinking, is valid and inspiring. We should analyse Information not only beyond the techno-centric and mechanistic view, but also beyond the other unilateral fixations. For example, within the Mind metaphor (the Direction perspective) there often is an attempt to claim that all Information exchanges can be explained as economic processes. Neoclassical economics, for example, is used to explain information as a set of economic phenomena.⁴⁴ In the mind of the neoclassical economist, all human activities employing any type of “scarce resources” can be addressed within a “price theory.”

Finally this means that all information activity is transactional, similar to commodity exchange, but if information is reduced to exchange, we are clearly moving within the Mind metaphor. Should we stop and reflect before if this is the only valid perspective on information? An extreme formula of this is to say that information is that which reduces uncertainty for the firm (i.e. knowledge capital), and we often participate in discussions where the “business side” will recognise as information only that which reduces uncertainty from their point of view. Every other interpretation, including the one governing the Mechanism metaphor, does not make sense. So in business, in academy, in technology and in corporate teams, we find these unceasing oppositions, sometimes in dialogue, sometimes in conflict with each other, but always without an insight of what is driving these differences, only to be resolved by accident or sheer power.

More than People, Process, Technology

I want to elaborate now how I think that we need to evolve beyond one-sided views in IT and Security management. In techno-centric environments it is not rare to find a strong emphasis on the idea of combining "people, process and technology." These are three aspects consistently covered by presentations, papers, books, proposals and reference materials, and these are considered the mark of a “good” approach to information technology.

This emphasis is shared by the major consulting firms and market research organisations. Business management wants to hear this approach when addressed, as a good signal of the knowledge of the consultant. All of this is true, but it is important to remark the emphasis on the three aspects is a late development in the IT world. Before that, a change that started around the mid-1980s, IT technologists did not use this discourse. The new emphasis represents progress in relation to a period when IT

disciplines ignored "people" and "processes" and when system analysis and design happened almost only in technique.

It is good to see an extended coverage of "people" and "process" in addition to technology. This amounts to some "moderation" of the mechanistic paradigm. In large organisations, deeply influenced by consulting services and market analysts, this "triad" of people, process and technology is also a given, something that managers will demand from their subordinates as if it were a sufficient condition of completeness and good practice.

So, complying with this, almost everybody in the industry works out carefully what the "people," "process," and "technology" factors are in any situation. Neat diagrams show how the advisor/consultant is covering "all the bases." Is this satisfactory? Is it "complete"? My view about IT and Security management is that we need to cover at least four aspects, and not only three. Perhaps this will be facilitated if we show that there is after all a certain approximation of the people-process-technology "triad" to the more complete model of the Four Perspectives:

- **The "People" concern maps to the disciplines of Verification and Selection**
- **The "Process" concern maps to the disciplines of Selection and Verification**
- **The "Technology" concern maps to the disciplines of Protection**

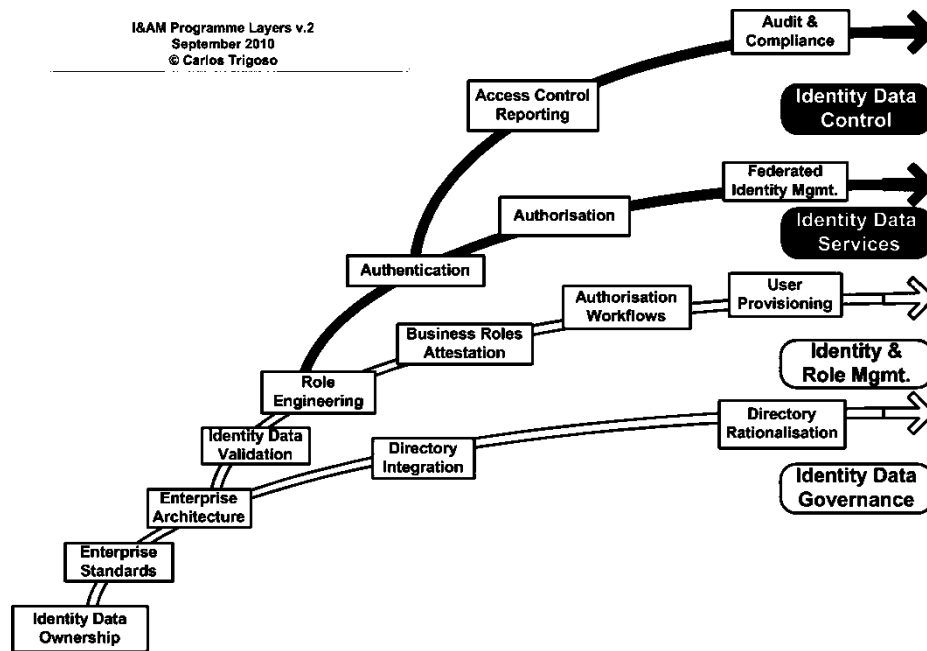
The concept of "People" is generally understood to cover the roles and rights needed for the users of an information system, but also the issues associated with people training and compliance. The concept of "Process" covers compliance with permission models, but also the authorisation mechanisms implemented in the organisation. And finally the concept of "Technology" addresses the hardware and software that provide access control, data storage, and networking and transaction capabilities.

This people-process-technology approach, although better than previous stances, is incomplete as it does not encompass the disciplines of Direction, i.e. it does not cover organisational factors which can be described and addressed only in terms of purpose, strategy, intention, ownership, authority, business model and risk-taking. This is noticeable when we speak about Security and Identity management. In this space, if we limit ourselves to analysing factors related to "people, process and technology," we will be unable to determine the goal of the Identity solutions. We may still cover the mechanical aspects of "provisioning" people, "controlling access" to systems, and "ensuring compliance," but we will be unable to explain why data ownership, business model and enterprise architecture are so important. Above all, we will be unable to answer the simple question: Why do we need Identity management at all?

If we adopt a techno-centric Identity management model, we could perhaps map every possible activity and workflow by using diagrams and models, perhaps with the help of some software tool capable of simulating human workflows. This certainly looks impressive on the screen and on paper, but the approach fails as the implementers do not realise that a technical solution does not represent the totality of the Identity management space. All processes around role management and role-centric

policies have at their core "business functions," "ownership constraints," and "authority factors" (here I use my own terminology), which cannot be described as process flows (for example in standard languages like Business Process Execution Language or BPEL). Organisational functions that correspond to the Direction and Selection perspectives, therefore, remain disconnected from the Security and Identity architecture, devoid of governance and are effectively abandoned by the business teams.

In 2010 I published a diagram showing how the different layers of Identity management relate to each other and especially highlighting the fundamental roles around data ownership and governance.⁴⁵



I&AM Programme Layers © Carlos Trigo 2010

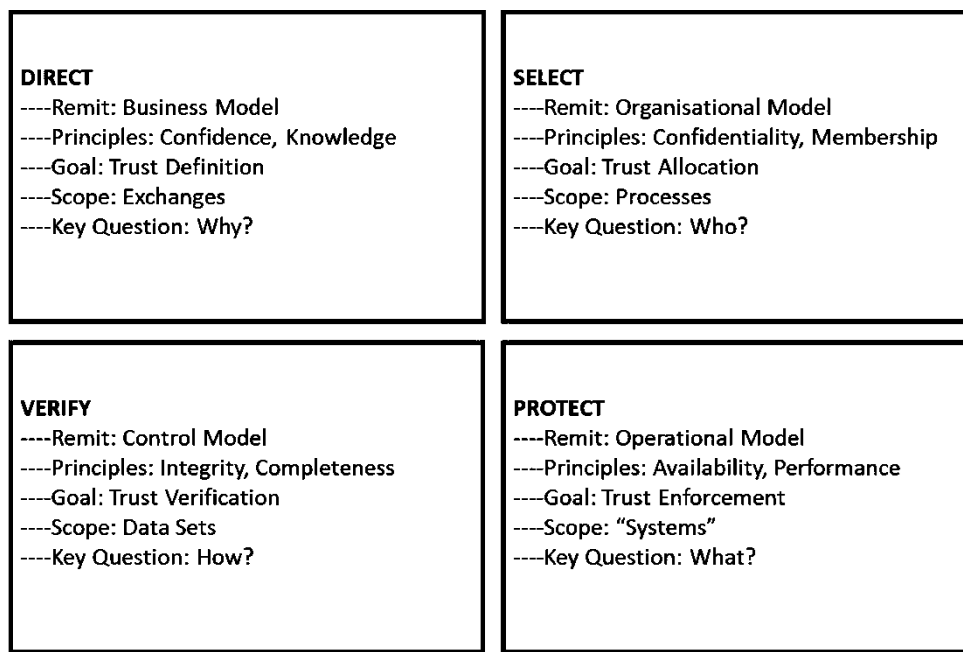
The four Layers are aligned to the four Perspectives: Identity Data Governance represents the Direction Perspective, while Identity and Role Management, Identity Data Services and Identity Data Control represent the other three Security Perspectives: Selection, Protection and Verification. In this way I showed how the logic of opposition can serve in fact to design and carry out a coherent organisational Security strategy avoiding one-sided choices.

The extended model, then, represents the integrated view of the disciplines of Direction, Selection, Protection and Verification. A detailed application to Security management as a whole is shown in the Annex to this chapter. There I show the Perspectives of Direction (Formism or the Mind metaphor) as articulated with Trust Definition; Selection (i.e. Organism) supporting the concerns of enablement, adaptation, decentralisation, membership and participation, also encompassed by the notion of Trust allocation; Protection (i.e. Mechanism) leading the search for resiliency, performance, fault-tolerance, redundancy, replication, perimeter security, and related efforts; and Verification (i.e. Contextualism or

the Template metaphor) associated with the detection of illegitimate/legitimate access and use, and compliance with laws and policies.

The goal here is not a simple match of the categories but using the root metaphors to clarify the specific points of view that are at play in the IT and Security professions so these may change and achieve higher purposes.

Annex to Chapter 9: The Security Perspectives



Summary of the Four Security Perspectives⁴⁶

¹ A radar chart or spider chart plots the values of each category along separate dimensions that start in the centre of the chart.

² J.R. Williams, G. F. Jelen, "A Framework For Reasoning About Assurance"- Arca Systems, Inc., 1998

³ Following Rudolf Kaehr's interpretation of Gotthard Gunther, "Each single value and each single logical function is entitled to have a logical meaning." See:

<http://www.thinkartlab.com/pkl/lola/Transjunctional%20Semiotics/Transjunctional%20Semiotics.html>

It is absurd to chase for the meaning of logical values and functions for arbitrary many-valued systems. Special value classes of some interest had been studied by logicians for 2, 3, 4, and infinite.

Hence, a method, like the arithmetic position system which is able to determine arbitrary numbers on a finite base system, has to be invented. This was Gunther's approach to many-valued place-value systems (Stellenwertlogik).

⁴ The Wallace Hypothesis: "...The hypothesis, which we shall call the "26 rule," is, then, that irrespective of race, culture, or evolutionary level, culturally institutionalized folk taxonomies will not contain more than 26 entities and consequently will

not require more than six orthogonally related binary dimensions for the definitions of all of the terms. ...In the area of cultural semantics, we are suggesting that a somewhat similar principle applies...the evolution of cultural complexity is limited, in so far as folk taxonomies are concerned, by the two-to-the-sixth-power rule. ...What is limited is the complexity of the taxonomies which are components of the various cultural sub-systems" A.F.C. Wallace "On Being Just Complicated Enough," 1961

⁵ "It all depends upon where the consciousness places itself and concentrates itself. If the consciousness places or concentrates itself within the ego, you are identified with the ego -- if in the mind, it is identified with the mind and its activities and so on. If the consciousness puts its stress outside, it is said to live in the external being and becomes oblivious of its inner mind and vital and inmost psychic; if it goes inside, puts its centralising stress there, then it knows itself as the inner being or, still deeper, as the psychic being; if it ascends out of the body to the planes where self is naturally conscious of its wideness and freedom it knows itself as the Self and not the mind, life or body. It is this stress of consciousness that makes all the difference. That is why one has to concentrate the consciousness in heart or mind in order to go within or go above. It is the disposition of the consciousness that determines everything, makes one predominantly mental, vital, physical or psychic, bound or free, separate in the Purusha or involved in the Prakriti." Sri Aurobindo, Letters on Yoga, pp. 235-36

⁶ Carlos Trigo, "Security Perspectives" - <http://carlos-trigo.com/public/security-perspectives/>

⁷ Carlos Trigo, "Four Perspectives on Risk and Trust" - <http://carlos-trigo.com/public/four-perspectives-on-risk-and-trust/>

⁸ Steven Palmquist, "The Combination Of Analysis And Synthesis In Numerical Symbolism," <http://staffweb.hkbu.edu.hk/ppp/gl/GL5.html>, and "The Geometry of Logic," <http://staffweb.hkbu.edu.hk/ppp/gl/toc.html>

⁹ S. Palmquist presents the following classification:

- 1 = end point of synthetic integration
- 2 = first level of analytic division
- 3 = number of steps in the process of simple synthetic integration
- 4 = number of elements in the second level of analytic division
- 5 = combination of 2 and 3 as found in natural organisms (addition)
- 6 = combination of 2 and 3 (multiplication) as found in inorganic systems
- 7 = logical systemisation on a higher level as a dynamic combination of 3 and 4
- 8 = number of elements in the third level analytic division
- 9 = number of steps and elements in the operation of second level synthetic integration
- 10= perfection of the number system
- 11= symbol of imperfect system
- 12= perfection of logical systemisation on the level of a single system (3 x 4)

See: <http://staffweb.hkbu.edu.hk/ppp/gl/GL5.html>

¹⁰ G.W.F Hegel, "Wissenschaft der Logik," 1812,

¹¹ C.S. Peirce, "The Categories," 1893

¹² I. Kant, "Critique of Pure Reason," 1781

Kant's table of judgments lists of the possible logical forms of propositions:

- 1.Quantity: Universal, Particular, Singular.
- 2.Quality: Affirmative, Negative, Infinite
- 3.Relation: Categorical, Hypothetical, Disjunctive
- 4.Modality: Problematic, Assertoric, Apodictic

¹³ Martin Heidegger, "The Thing," 1950

¹⁴ Chris Lofting, "The Neurocognitive Roots of Logic," 2003 - <http://www.emotionaliching.com/myweb/logic.html>

¹⁵ Anthony Judge, "Laetus in praesens" – Website: http://www.laetusinpraesens.org/bio/faq_laet.php#A5

¹⁶ W. McWhinney, "Paths of Change: Strategic Choices for Organizations and Society," 1992

¹⁷ George A. Kelly, "The Psychology of Personal Constructs," 1955

¹⁸ See: Adi Masli, Vernon J. Richardson, Marcia Weidenmier Watson and Robert W. Zmud, "CEO, CFO & CIO Engagement in Information Technology Management: The Disciplinary Effects of Sarbanes-Oxley Information Technology Material Weaknesses," 2009

¹⁹ See: Natalia Mintchik, Jennifer Blaskovich, "The Role of Politics and Institutional Isomorphism in the Decision to Outsource in the Post-SOX Environment," 2008

²⁰ The Sarbanes–Oxley Act, 'Public Company Accounting Reform and Investor Protection Act' and 'Corporate and Auditing Accountability and Responsibility Act', 2002

-
- ²¹ Aki Iskandar, "Butting Heads: Why IT and Business Don't Get Along" www.LambdaSoftware.com
<http://www.oracle.com/technetwork/articles/entarch/iskandar-butting-heads-487873.html>
- ²² In his book "Does IT Matter?," Nicholas Carr quotes Richard Veryard: "Thanks to the plug-and-play business approach, a new business can be rapidly assembled as a loosely coupled set of partnerships and services [...] even a substantial company can now be viewed as a component of a much larger system, rather than as a self-contained business operation," R. Veryard, "The Component Based Business: Plug and Play," 2000
- ²³ Richard Jung, "A Quaternion of Metaphors for the Hermeneutics of Life," 1985
- ²⁴ R. Jung writes: "My second thesis is that although the four metaphors seem to be contradictory if treated as ontological statements about the nature of living systems (and thus the opposition of any two of them gives rise to an unsolvable paradox) — the paradoxes are dissolved when each metaphor is treated as a different matrix for expressing different epistemic attitudes." — "A Quaternion of Metaphors for the Hermeneutics of Life," 1985
- ²⁵ S. C. Pepper, "World Hypotheses: A study of evidence," 1942
- ²⁶ John Arnold, "Security Services Model," 2006
- ²⁷ Magoroh Maruyama, "Mindscapes, Individuals and Cultures in Management," 1993
- ²⁸ Alessio Moretti, "The Geometry of Logical Opposition," 2009 -
<http://alessiomoretti.perso.sfr.fr/NOTMorettiPhD2009GeometryLogicalOpposition.pdf>
- ²⁹ <http://alessiomoretti.perso.sfr.fr/NOTSchang.html>
- ³⁰ <http://alessiomoretti.perso.sfr.fr/NOTPellissier.html>
- ³¹ <http://alessiomoretti.perso.sfr.fr/NOTSmessaert.html>
- ³² Jean Piaget, "Traité de logique. Essai de logistique opératoire," 1972
- ³³ Walter Helbig Gottschalk, "Theory of Quaternality," 1953
- ³⁴ "You see that by still preserving this "like" (comme), I am staying within the bounds of what I put forward when I say that the unconscious is structured like a language. I say like so as not to say-and I come back to this all the time-that the unconscious is structured by a language." Jacques Lacan, "The Seminar, Book XX: Encore, On Feminine Sexuality, The Limits of Love and Knowledge," 1998
- ³⁵ The home page of N-Opposition Theory : <http://alessiomoretti.perso.sfr.fr/NOTHome.html>
- ³⁶ Anselm was born in Aosta, in the kingdom of Burgundy. In 1033, at the age of 27, he joined the Abbey of Bec, where he served as abbot from 1078 to 1093. In 1093 he was made Archbishop of Canterbury.
- ³⁷ Sara L. Uckelman, "Anselm's logic of agency" Institute for Logic, Language, and Computation, 2009 and Douglas Walton, "St. Anselm And The Logical Syntax Of Agency," Franciscan Studies, Vol. 36, 1976
- ³⁸ Anselm's work on logic can be found in the "Complete Philosophical and Theological Treatises of Anselm of Canterbury," translated by Jasper Hopkins and Herbert Richardson, The Arthur J. Banning Press, Minneapolis
- ³⁹ Gurpreet Singh Dhillon, PhD Dissertation, Department of Information Systems, London School of Economics and Political Science, December 1995
- ⁴⁰ Gareth Morgan, Gibson Burrell, "Sociological Paradigms and Organisational Analysis," 1979
- ⁴¹ Gurpreet Singh Dhillon, PhD Dissertation, Department of Information Systems, London School of Economics and Political Science, December 1995
- ⁴² R. Hirschheim, H.K. Klein, "Four paradigms of information systems development" , 1989
- ⁴³ D. Sholle, "What is Information? The Flow of Bits and the Control of Chaos" - <http://web.mit.edu/comm-forum/papers/sholle.html>
- ⁴⁴ Joseph Stiglitz, "Information and the Change in the Paradigm in Economics," 2001.
- ⁴⁵ Carlos Trigos, "I&AM Programme Layers," 2010 - <http://carlos-trigos.com/2010/09/12/iam-more-than-people-process-and-technology/>
- ⁴⁶ Carlos Trigos, "Security Perspectives 2012"- <http://carlos-trigos.com/public/security-perspectives-2012/>

10. The Cloud Transition

Security Arguments are Philosophical

How moral is a technical dilemma? How technical can a moral argument be? Philosophical questions are rare in Security-focused debates unless people are trying to make a “political” point, i.e. a critical point about technical choices. Usually in these cases the choices are about what is deemed “better” or “more advanced” in technological terms, and not about truth or ethical questions. The root of this problem is that Security lacks a theory, as I wrote in a previous chapter. We have principles and “best practices” but we do not have a theory explaining our actions “from first principles.”

Would such a theory be possible? In this book I have shown some examples of how the current Security approaches rely on ideas and presuppositions that can be identified as a form of mechanistic ideology. I pointed to the problems arising from Information thought as an object and Security centred on protection and defence of “information assets.” A philosophy, though, would take this trend as part of reality, as a “perspective” and correlate it to other lines of action and thought.

From protection-centric Security we would be moving logically to user-centric and data-centric alternatives, not to discard the dominant ideology altogether, but to put it in context and help free our thinking and our actions. For Identity management, we would see for example that we need to offer a new vision by joining “analytical” and “synthetic” approaches instead of following the latest marketing trends.

How moral is a technological question? In the current era, technological discussions are essentially philosophical ones, even if we don’t see that. Or, better said, current technological issues are our modern philosophical debates, disguised as empirical choices. This view has multiple results for the present and the future, and I will explore some of these in this last chapter.

Cloud Computing and the Problems of Information Technology

Cloud computing is a new step in organisational and social history. It is rooted in the changes driven by profit maximisation, global leverage of salary differentials, new levels of division of labour between countries and within these. Organisations adapt to these global changes, rapidly losing any national or local character and adopting technologies that speed up this post-cultural transformation.

If at first organisations adopted Information Technology as a differentiator, seeking commercial advantages that were promised by the new technologies, further adoption has been hampered by problems. Information Technologies transformed rapidly into commodities and the assumed advantages disappeared. Frequent and severe IT project failures are only the backdrop to a deeper problem, which was the opaque relationship between technology adoption and corporate productivity. Nevertheless, despite the obstacles and problems, IT adoption continues at a fast pace. This helps to

see that at the core of its social and economic role the driving factor is not the technology itself, but the work and the workers that act with it and through it. The generic “information worker” is the real force behind the mysterious “success” of Information Technology in the face of unlikely and elusive benefits derived from its adoption. Value, when it comes, is generated by the new universal, transnational work (essentially services) and not from any particular technology. This is why positive correlations between IT investment and enterprise productivity appear only when the organisation has other programmes in place, hiring, enabling, educating, freeing and leading the new working classes of professionals. When this is not the case, IT investment by itself fails to produce any value for the organisation, and the same is the case with Information Security and Identity Management investments.

These underlying causes explain too why Information Technology and Security professionals are confused and sometimes resistant to the global adoption of Cloud services. Businesses enter into the “Cloud Transition” phase when investments in IT can be conveniently replaced at a fraction of the cost by external capabilities. At the same time, the only differentiating factor that remains is the ability of organisations to leverage skills, creativity, education, mobility, dynamism, and ambition of their people.

Business continues to evolve

Business organisations are increasingly adopting outsourced IT services and the use of externally hosted infrastructures. For those organisations that didn’t make the change consciously or still move through a hybrid phase, a new problem appears as the variety and complexity of user administration and user access rights becomes very difficult to manage.

What are the differences? What can help organisations draft suitable Security policies? While there are still differences related to business models, we can see the same groups of users across many private and public sectors, all showing similar needs. The signature of these changes is that users previously considered “external” have equal or more access needs and rights than “internal” users. Complementing this, “internal” users also interact with the organisation as “external” customers and citizens. This leads to a new panorama where traditional “enterprise” approaches and IT “solutions” cannot and should not be devised separately from all other forms of “identity management.” In writing this I am consciously adopting the view there is no Security strategy that is not an Identity management strategy in essence.

Amid this change, technologists and managers have to recognise their way of acting has to adapt. Sometimes, terms that appeared in other contexts are used for the Security practices. This is the case of the Service Orientation born in the period where the emphasis was on enterprise-level software and database development. Now this terminology is used –I think properly—for the Security and Identity specialities. For about 10 years now some experts have been writing about Security and Identity “as a Service.” The move into the Cloud has given more energy to these calls for transformation, but the results have been so far incomplete.

The Cloud has many aspects, but it tends to appear as one thing in particular for those who approach it within the traditions of the computer revolution of the 20th century: the Cloud phenomenon appears as an incarnation of the out-sized computer, sitting somewhere remote and isolated, capable of everything, ever-present. Cloud computing is thus understood as a return to the mainframe era, a fact not ignored by hardware vendors who are continuously trying to “run the Internet” on some collection of multiprocessor “boxes.”

To the hammer, everything looks like a nail, as the saying goes, and that is how people see the tools and technologies around the Cloud, and by doing this, the conventional observer misses the fact the Cloud is not (and can't be) a technological compound, but essentially reflects historical and sociological changes, a different context to the one where some of us learned to use the Personal Computer.

This is the case with those disciplines like Identity and Access Management which are tightly related to organisational, non-technical causes. To the techno-centric practitioner, Identity management –even when based in the Cloud-- is frozen in time at the moment somebody thought about the possibility of centralising user control across many separate machines and operating systems. Currently the Identity management experts are still fixated with the technologies of “user provisioning” and “role management” as these were elaborated during the Mainframe and later Client-Server periods.

Supported by this fixation, the most notable change in the technology market has been the reduction in the number of technology suppliers, ending in a small core of large, monolithic offerings which compete more on size and difficulty of implementation than on effectiveness and business value.

Under the spell of these technologies, Security and Identity specialists think more of complex platforms and extensive software development tools this time offered “in the Cloud,” or as “Software as a Service” (SaaS). The change ends there, because these conceptions are an obstacle for the Security disciplines and for Identity management in particular, as professionals limit their work to models that have little to do with Identity and the possibilities of the Cloud. Not only the social and economic nature of the Cloud is lost, but also the wrong tools are adopted for a reality that does not lend itself any more to the traditions of “enterprise architecture.”

As this model fails and the number of abandoned “provisioning” projects grows across the world, surprisingly the technology market starts to fragment again, moving away from the previous concentration in the hands of a few sellers. Some new entrants follow the SaaS model to offer parts of the Identity technologies, while others remain “in the enterprise” and focus on the areas of “risk-based reporting” and “compliance.” In the whole, this fragmentation is positive for business leaders and consumers in general, and it is safe to predict the rapid loss of relevance of the “end-to-end” Security portfolios. As part of this development, I predict an increased focus on the core of Access control, i.e. the disciplines of Authentication and Authorisation, and a move away from the focus on “provisioning” and “role management.”

Traditional thinking focuses on Unique User IDs, password management, well-defined roles and “user provisioning,” and more recently on risk-based reporting and application per application access

control, but all of this will give way to new forms of Identity management that will challenge at the same time the monolithic “platform” approach, and the “niche vendor” approach.

These will not be vanquished by a new technology, or the “next big thing,” but fundamentally by a new way of doing things across computing networks. The new technologies will be the product of this new period, not the cause of it, and the inventors of these new technologies will be the interpreters of the economic and social change that is driving all of this. As I have been describing in this book, what is new in Identity stems from post-industrial, post-cultural, capitalist, globalised commercial exchanges and human movements. The forces that cross and surpass national boundaries and transform the family and local life, also change business and organisational structures.

The global, transnational enterprise is also global in the sense that it represents the existence and reproduction of identities that are mobile and rootless, lacking firm context and defined loyalties. These “identities” are abstractions of biological individuals, “equal individualities” and entities with little history and references to begin with. No individual appears certified, but only as a fragment of a legally existing person, and only as a function or a partial activity in the economy or as part of an organisation. In the global network, the activities of the individual are indirect and partial, or better said, a shadow of a real individual.

For this fundamental, non-technological reason the monolithic individual does not exist, and therefore in dealing with Identity we are not facing a definable object, but an activity. Professor Chadwick,¹ a prominent British scholar in the speciality of Identity management has formulated this synthetically with the formula: “It does not matter who you are but what you can do.”

Global and national organisations cannot rely, and should not rely, on unique identity instruments (credentials) or stable identities. They should aim instead at defining, enabling, protecting and verifying stable modes of informational exchange and access routes. The key to Cloud value is a “variety of identities.” Unique, flat, general and shared network spaces with stable identities are things of the past.

Now, in this context, something is still missing, and is still difficult to grasp if we stay with the technocentric perspective. For the individual as a natural person, his or her “identity” continues to be unique and coherent, even if it is partial and unstable for the multiple organisations, contexts and realms he or she moves in. For the organisation Identity is fragmented, scattered but still falsely understood as unique and defined.

This is the contradiction that we live in, the ideological framework that makes us think of Security as a profession bound to protect and defend; while it should be clear to all that we are missing the point and not responding to a historic challenge with such attitude. In fact, understanding that it is sociology and history which drive change and not technology would lead us to see the whole promise of the new era is rooted on widespread individual use of computers, a new form of generalised work. The machine is the instrument and the mediator, but the machine is only responding to expanding human action. It

is this mediation that allows for anonymity and hence creates the context of fraud and crime (because it underpins the context of freedom).

In seeing this, the controlling “protecting” technocratic spirit tries to turn against the basis of the historical period and tries to cancel anonymity as if it were some accidental unwanted feature in the current situation. This ignores that computing power in the hands of individuals and indirection of personal activity are the foundations of the digital global market. This market is indeed the product of uprooted, universalised, generic, global indirect activity that is not materially linked to the biological person (to the taxpayer, the homeowner, the corporate worker), but only indirectly and voluntarily so.

Is it not the case then that linking back all activities in the network to the “real biological person” is not only impossible but also counterproductive? Besides, is it not the case that successful business models always arise without such linking? Here is my thesis: fragmentation of the identity is not a problem if a) the person has the power to decide to act through the network; b) if multiple identities, i.e. levels of action are acceptable for the business models; and c) if various identities (and channels) are acceptable for commercial exchanges and human interaction in general.

False perspectives disappear once we understand that technologies create their own justification and present themselves as “causes” when they are not. Technologists and conventional Security experts cannot see that indirection and abstraction implicit in the computer create indirect mediated action and abstract, uprooted shadows of the individual, and not the other way around. Is it a serious stance to detest the unnamed anonymous “hacker” that is enabled precisely by the techniques of remote computing? Is it a rational stance to alert of the risks of “attacks” to data just when we expose data to the global networks?

If we think of these problems for a minute, we will immediately see that the risk of fraud and impersonation, as well as all other Security “problems,” are derivatives of multiple layers of indirection in commercial and social transactions through the computer networks. Shouldn’t it be obvious the way “forward” should not be to plan the rest of our lives as a war against masked aggressors, “exotic” hackers, and “anonymous” enemies but to adapt to this new context? Our commitment should be instead to develop new protocols, new assurance levels, new business plans, new strategies and various identities on all sides, across all boundaries.

Specifically: a variety of identities means parallel or shared identities and concurrent flows of collaboration managed by the individuals. The new model is one where Identity management is not and cannot be a gubernatorial discipline to bring order where there is chaos, to simplify where there is complexity or to reduce choices where there is freedom. I also imagine the moment where Identity management will stop being seen as part of Security and become just one more art of business risk-taking.

Eclosion of Security Concepts

When I meet with senior Security experts, especially those in upper management positions in public and private organisations, the conversation often focuses on the future of Identity and Security

management. I confess that this is a subject of constant reflection for me and I eagerly take part in such exchanges when the opportunity arises. In these discussions I see that Security and Identity management leaders face every day complex decisions about their organisations, as these evolve and address new problems in the global network.

The consensus usually is that Security and Identity management cannot be delivered any longer purely within the boundaries of the organisation or enterprise, and that new ideas are necessary to face the challenges that come with de-perimetrisation and Cloud Computing.

In considering the subject, it is compulsory to leave behind either a pessimistic or a naive optimistic stance: either believing the future will be “more of the same” or “completely new.” These are false assumptions. What we see --both in technology and business practices-- is that the new coexists with the old, and the old gives birth to the new. The combined result of these movements is what I call “eclosion” --from the French *éclosion*-- meaning “to hatch” or “be hatched” -- using an image from the biological sciences.

In a more descriptive way I like to think of change not as evolution or displacing one class of systems by another, but as the constant unfolding and opening of reality. Here, to avoid an excessively wide discussion of these matters I want to focus on the plane of conceptual transformation and for example on the changes driving Security and Identity. In the realm of ideas, we should speak of “differentiation.” The following trends were presented in chapter 6 and are repeated here for convenience:

- The protection and compliance focus which Identity management inherits from the Security Domain will not disappear, but it will have a lesser role in the IT landscape than it has now.
- Centralised control models over identities will be reserved for restricted areas of the IT infrastructures, while organisations implement federated and decentralised assurance services.
- Privacy and Data Protection concerns will be seen as essential, but increasingly not as a central management task, and instead as rooted on the individual choices and different varieties of identity.
- Identity management as a Service will experience rapid adoption but a single model will not exist, and corporations will sometimes have partly hosted and partly on-premises solutions.
- The intellectual structure of Security and Identity management will change, moving from a focus on Risk Management, to a balance of Risk and Trust Management.
- Given the perceived and real risks of network crime and disruption, security will rely even more on defences in-depth, and a variety of identities and identity assurance levels while using more refined risk-based and attribute-based access controls (all of this enabled by Identity management solutions).

Each of these trends has in itself a counter-balancing element which on the one hand represents a continuation of the past, but also is a reformulation of it. Change by differentiation leads to increased complexity.

Cloud Computing is not itself caused by changes in Security or Identity disciplines, but, as I explained, the latest stage of a trend that has been always present in computing towards virtualisation, shared

capabilities, resilient remote resources and networking. The Cloud is at the same time a continuation of the old and the appearance of new and different models of infrastructure and application services. This has an important effect on the future of Security and Identity management.

In developing Cloud computing, we see two major trends arising: Identity management “for” the Cloud, and Identity management “in” the Cloud. The first represents Security services to protect the Cloud environments themselves; and the second is the Identity services offered from Cloud or hosted platforms. The two types of service are inseparable but need to be distinguished in our study.

Security and Identity “in” and “for” the Cloud reflect two “views” among the users of these services and IT specialists: Security for the Cloud means securing the broader IT application and data workloads as they migrate from corporate data centres into Cloud services. Security in the Cloud means developing a new delivery model for IT solutions - for example, Identity management as a service.

The core of the conceptual differentiation taking place at this level is between Trust and Risk Management. On the one hand, Security in the Cloud is a view that reflects the ideas of Trust Definition and Trust Establishment, leading to a stance centred on Trust Management. In this “world” Identity is seen as Distinction and Membership. On the other hand, Security for the Cloud is a view that reflects the ideas of Trust Enforcement and Trust Validation, leading to a stance centred on Risk management. In this “world” Identity is seen as Object and Context.

These views represent different action perspectives and different participants: For Security in the Cloud, we have the Subjective position, the position of the business owner and leader, the strategist, but also that of the group, the organisation, and Society in general. In Security for the Cloud we have the Objective position, the position of the implementer, the controller, the auditor, but also that of the engineer, the technologist, the IT organisations in general.

Trust Definition and Trust Establishment are crystallised in a view of Security “in” the Cloud, and answer the question: How do we benefit from operating in the Cloud; how do we manage trust with our clients, colleagues, staff, partners, etc. Trust Enforcement and Trust Validation are at the root of a view of Security “for” the Cloud, seeking assurances for Data Control, Compliance, Protection and Privacy. It is obvious these views are complementary. It is also clear the two major groupings here described can be analysed further into the four perspectives that I have presented in previous chapters:

- Trust Definition: Security seen from the perspective of Direction and Identity seen as Distinction.
- Trust Establishment: Security seen from the perspective of Selection and Identity seen as Membership.
- Trust Enforcement: Security seen from the perspective of Protection and Identity seen as Object.
- Trust Verification: Security seen from the perspective of Detection and Identity seen as Process.

The delivery of Security “in” the Cloud is a precondition for realising Security “for” the Cloud. An excessive focus on security “for” the Cloud assumes the organisation is not yet benefitting from these capabilities and needs assurances to adopt Cloud-based solutions; while the view focused on security

“in” the Cloud seems to reflect the target state of any Cloud initiative: security as a service “in” the Cloud.

While the two views remain linked and dependent on each other, the Risk-centred “view” will predominate in the context of deciding how to adopt Cloud-based strategies; contrariwise, the Trust-centred “view” will predominate in the context of delivering or exploiting Cloud-based services. The two views are part of the same panorama and have to be mastered in the Cloud Security strategy. Because of this, it is advisable to keep in mind the disciplines of Trust Definition and Allocation are still not well developed and stay in the background among Security professionals. In the new world of Cloud computing, nevertheless, it is essential to develop a balance between these disciplines and the dominant perspectives of Trust Enforcement and Verification.

Setting up and governing Identity data ownership should be the base of Defining Trust between the participants in the market. Developing new protocols for the establishment of collaborations and partnerships, and defining employee, consumer, citizen and third-party access levels are at the base of the Establishment of Trust between the users and organisations.

It will be necessary to adopt a wider combination of policies, roles, groups, capabilities, attributes and credentials for such variety of users. This will enable them to access multiple channels within a number of levels of assurance around the enterprise and its partners. In the same way, standardising data, identity propagation and assurance processes will support the Verification of Trust.

Risk Focus and the Cloud

In day-to-day corporate management the easiest way to appear “on top of your subject” is to avoid contradictions when you speak. It does not matter if you know your subject, for in a generalised Services Economy and in Information Technology there are hardly any standards. When presenting something, the IT manager can survive by being consistent and conservative. For example, in speaking about security it is “safer” and simpler to think and act following the usual ideology that “everything in Security is about risk.” Your task is automatically cut down for you as you can focus now on “risk mitigation” and “managing security threats.” Security specialists will not challenge you, because we also move within an ideology that says: “Yes, we know that Security includes trust management, but we have decided to focus on Risk management and risk avoidance only, because ... we are specialists after all.”

These positions are protected by the assumption that to be objective, Security practitioners and experts have to be essentially Risk managers. Underpinning this self-perception, the Security profession thinks of itself not only as objective, but also as scientific and quantitative. When challenged, the Security expert will doubt that Trust can be measured, for example, and will try to prove that Risk is the only measurable “quantity” in Security. After all we have plenty of measurements and assessment methods, like the now-abandoned ALE², ROISI³ and the Gordon & Loeb investment functions.⁴ And don’t we have “accepted” practices around threat and risk probabilities?⁵

The Security expert convinces him or herself that those sub-disciplines not centred on Risk management are somehow less objective or less “quantitative” than they practice. It is usual to see the Identity management people as lacking in business insight because they recommend investments just based on organisational transformation and overall efficiencies. Have we not all learned in our training and certifications that Risk is the only objective measure?

In the same vein that I asked at the beginning of this chapter what is the moral bearing of a technological argument or the technological value of a moral choice, I have to ask now, philosophically speaking: What is subjective and what is objective? It is critical to clarify the use of terms here, because we take things for granted too easily, and assume that some terms have evident or definitive meanings. We need to make a distinction to fully grasp what we mean by these terms and determine how these can be applied to our profession.

To promote this discussion, I often suggest that we agree on a distinction between what is quantitative and what is not. In this way, we can arrive at a wider distinction, between the objective and the subjective. The intent of the objective/subjective distinction is comfortably matched by the quantitative/non-quantitative pair because, if a statement is quantitative, then it is communicable, and thus it can be corroborated by evidence. If a statement is not quantitative, then it remains in the realm of pragmatics, i.e. the Person. Therefore it is essentially incommunicable and remains beyond verification. In other words, the non-quantitative is necessarily subjective, while the quantitative has at least the change of verification. Only the Number (quantity) manages to cross the gaps between Persons, Subjects and Agents.⁶

In Security, what is quantifiable and what is not? We know the sorry state of our disciplines when it comes to assessing the value of our proposals, plans and solutions. Even when they insist on quantitative Risk assessments, our Risk managers are shy when it comes to show any success of security investments. Not only the industry but also academia and literature fail to show consensus about the value of Security and IT investment in general. In fact, although the IT world prefers to ignore this, to date the function and value of IT are not settled matters. This is even more the case in the face of quickening global changes. And the problem is wider: few experts would dare to explain the nature of Information itself, while so many of us still keep talking about the “value of information.” That has not been settled either: the concept of information has at least four different meanings in the literature: as an object, as an intangible value, as relationship and as process.

How is it then, given these flaws, that we do not see their effects in understanding Security? How are we still comfortable speaking about “Information Security” and about the “Identities” that access “Information”?

In the midst of the Cloud Transition, the Risk-focused managers like to fashion themselves as the most quantitative orientated experts, by using security breach and attack “statistics” and “threat modelling,” as well as “probability calculus.” Sadly, as we have seen in a previous chapter, all of this boils down to some experts choosing the weights of the factors and advising what threats are meaningful and which

ones are not. Instead of probability calculus we have some medieval theory based on “authorised opinions.”⁷

Further, especially because the whole world of Security is changing, we need to accept that it is even more difficult to show the value of IT investments themselves, and not only in Security or Identity management. We should face the realities described by Nicholas Carr in his 2003 article “IT Doesn’t Matter.”⁸

Quantitative Identity Management

It could be argued that decision-making about Identity management is difficult because of factors that are not intrinsic to the discipline, for example, related to the maturity of the business. I think that this approach evades the problem. After all, it should be always possible to present a good investment proposition even if the organisation does not have a grasp of the complexities of user management.

Of all the areas in Security, Identity management seems to be the least quantifiable (keeping the distinction that I proposed above). Now that some Risk experts dare to recognise the difficulties they have in showing the results of investment, there is perhaps some chance that the Identity specialty becomes more normal after all, but I do not think that we need to rely on a change in views at this point. The Cloud is bringing a different context. A formula may capture what is happening: Identity becomes more relevant, more material, when information becomes indirect. In a somewhat more detailed expression, I like to say that Identity becomes more objective (quantifiable) when the users exchange information more indirectly. This is easy to understand if we think that human exchanges evolved incrementally towards more indirection and abstraction, while in the past even “information exchanges” were only done between natural, physical, present individuals. As the separation evolves, Identity becomes less personal and more symbolic, mediated and numeric. In this sense, it becomes more quantitative.

This is the key to understand not only why Identity management appears first as the least quantifiable of the Security disciplines, but also how in the near future, this specialty will be the only quantifiable one, while the other areas still will need a longer travel in the Purgatory of “knowledge by experts” and “art practitioners.”

In a previous chapter (“Quantitative Identity Management”) I described how identity data flows can be isolated and assessed, and how these becomes symbols and agents of organisational work. Identity data is notoriously mismanaged everywhere. There are fundamental problems of governance, of standards, of architecture, of validation, authorisation and provisioning processes. Let’s be clear: these problems are not getting easier or smaller. Actually they are exploding and deepening as organisations of all sizes enter the third or fourth waves of globalisation. On this ground we should not only be thinking about the Cloud, but also “after the Cloud,” towards the next wave of indirection and human work abstraction.

In the recent past, even while client and user data was treasured and reasonably governed (either by reasons of commercial interest or via regulatory pressure), identity data was not only mismanaged, but

also not measured. It was never considered an “asset,” resulting in a situation where Identity data was the only major category of business-related data that was not managed, as if it had no value at all. From the micro-economic angle, though, it is clear that Identity data was not measured while it was chiefly “internal,” i.e. employee or direct contractor Identity data. These blocks of data were rationalised as non-asset, “worthless” informational entities about “cost factors” and not sources of revenue. In other words, even in the post-industrial enterprise, at the start of the current globalisation wave, Identity data that originates in “cost factors” was and still is considered as not being “an asset.”

It will take more work and research to discover all the related issues, but this already explains the current state of mismanagement of Identity, and the future of Identity in the period of Cloud transition. Data that remains rooted in “cost factors” will not be managed as an asset (by default); excepting those cases where enlightened management recognises the intangible benefits of Identity data management in the core enterprise and its immediate periphery. Contrariwise, other types of identities, originating from partners, collaborators, suppliers, distributors, and public and private consumers, will increasingly be treated as a series of complex “assets” deserving better or more effort into Identity management. Now, because the core enterprise is decreasing in absolute and relative terms anyway, and because the “external” users are many more than the “internal” ones, once better Identity processes become the standard, then we will see a rational cost-based solution for corporate staff. While the Cloud transition is unfolding, the real costs and negative impacts of defective user management processes and technologies is ignored by private and public organisations alike. User management costs are not even an item in IT cost schedules.

In other words, business change drives organisational change, and organisational change drives the utility of Identity data management. This is precisely the meaning of the Cloud Transition. Identity management is also transitioning from a sub-discipline focused inside the Enterprise (looking from the inside-out so to say), to a transformed praxis coming from outside of the Enterprise.

In this sense, in the measure that other Security disciplines remain anchored behind the firewalls and rotating doors of the corporate buildings, Identity management shall detach itself from Security in a very interesting way. From being something the IT department doesn’t want to do or was not ready to do, it will become something the IT department will never do. Around the same time, though, in a moment of revelation, IT experts will wake up to discover they themselves have ceased to have or to be a Corporate Department altogether thereby ending the long and fruitless try to “align with the business” as well as their tortured experience with Identity.

That will stop a constant tendency towards fragmentation of the Identity solutions, or “point solutions,” as we say in the trade.⁹ Everyone in the Profession sees user management as part of security, the same as everyone sees Security as part of IT. This is a wrong perspective. By doing this, we are taking distance from business, even if we promise “alignment.” This is so because current conceptions of secure user management are not where the reality is going, because security theories are incomplete in this space, and--note this--because Risk-based Security is essentially non-quantifiable and “subjective.”

Against the backdrop of the Cloud Transition, an objective (quantifiable) approach is not only necessary but feasible for Identity Data Management once we address transforming user types and user access routes described earlier in this book. By looking into these data flows as business data, we will not only articulate a discourse of value, but can also quantify the complexity, the change, the cost and finally the exchange value of this information. The enterprise will discover the full value of identity once it stops to own it. On this basis, we will see Security and Identity management as a question of performance, flow, network reachability and workflow efficiency and Identity Data will be a product, at a price, but not anymore a product of the transformed enterprise.

Facing Reality

Addressing the Cloud Transition means adopting quantitative Identity management in the global stage. While in the past good Identity management—always an unreachable goal—was predicated on internal business processes, in the new period a completely new rationale is coming to the fore whereby “good management” is not and cannot be internalised management of external identities.

Let us summarise the obstacles that existed even before the Cloud became an economic and social imperative. Most of these factors are either ignored or “hidden” from view within the dominant techno-centric paradigm:

- Hidden costs of IT Operations and project delivery (project mobilisation, project delays and failures, IT inefficiencies)
- Undue and unexpected, un-evaluated effects of outsourcing arrangements (internalised management of external identities, inadequacy of traditional technologies in the deperimetrised enterprise)
- Continued divide between IT and business departments (persistent lack of alignment and absence of common objectives)
- Persistence of risk-based security and risk-focused investment decisions (under- and over-investment in technologies)
- Limits induced by a problematic theory and understanding of “information” (excessive costs and deficiencies managing information as an “object” and not as a process)
- False definition of future stages as “simpler” or “less complex” (wrong expectations of business and IT teams assuming complexity can be “reduced” with more technologies)
- Investment and commitment tied into monolithic Identity technologies and network operating systems (technologies designed for enterprise, closed environments slow down organisational transformation)

More specifically, in the Security and Identity areas, conventional approaches lead the business teams and technologies to focus on:

- Centralisation of access control
- Automation of identity life-cycle (push model)
- Educational activities focused on “compliance”

- Compliance focused on vulnerability patching
- Access control taken as access remediation (account cleaning)
- Risk-based reporting defined as “detection of misbehaviour”

We have seen already the roots of this direction. It suits a vision where the essentials are:

- Operational costs
- Financial losses
- Perception of exposure to “Security risks”
- Regulatory Compliance
- Number of breaches, incidents

In this context, inevitably, all Security becomes equal to “protection.”¹⁰ As a result of this all our activities are articulated around the “pressures” that IT managers experience in their jobs. All solutions become technological choices between “tools” and the primary selection criteria are savings, reduction of service desk calls, decrease of effort in account management, “simplification of processes,” savings in compliance cost and related measures. In other words, Security becomes an IT matter, to be owned and resolved by IT managers and experts. Just considering this end scenario leads us to see how absurd the starting point is.

After The Clouds

To leave behind this fruitless state of mind it is necessary to “transition to the Cloud” but with clear vision. It is essential to avoid adopting the Cloud as another technology in the hands of the old IT Department. An example of continuing old prejudices can be seen in the polemic exchanges taking place between Larry Ellison and Marc Benioff, respectively CEOs of Oracle Corporation and Salesforce.com, in the past few years. This debate was summarised by Bob Evans writing in Forbes Magazine.¹¹ Computerworld and InformationWeek carried at the time good descriptions of the discussion.¹²

The Web is full of exchanges like these, where marketing strategies are confused with analysis, and the discussion becomes a distraction, if not even the cause of more confusion, for the business and technical leaders considering Cloud adoption. In this debate, for example, the terms “false cloud” and “real cloud” were used liberally.

Terms like “false cloud” and “real cloud” mobilise underlying subjectivities and commitments but are not rational arguments. To begin with, there is nothing like a “false cloud” or a “real cloud.” The Cloud is not coherent, finished or complete; it cannot be defined once and for all. It is not only still in the making, but also it is essentially not of a technical nature.

We can see that many discussions about the Cloud (and the Ellison-Benioff debate was no exception) set comparisons around technical capabilities like “virtualization,” “efficiency” or “Java-enablement.”

That is precisely the discourse of the old IT Department. To be fair, in this debate Benioff did make very good points, addressing non-technological qualities of the Cloud—saying for example that it has to be “democratic” and “economic.”

Technical differentiators are fine, and each technology house will have some technical solutions, hopefully well-integrated into their offerings, but Cloud consumers (either companies or individuals) should not get distracted by these functionalities or impressive hardware specifications, because the Cloud is above all a social and historical phenomenon. The roots of this phenomenon are economic in nature, and they are global, but the technologies and principles are not new. These existed since the start of the electronic computing era and were not invented recently as many experts believe!

It is the global extension, the variety of user types, the diversity of applications and services, and exploding business models that makes the Cloud. Benioff’s Salesforce is not less “true” than Ellison’s database in the Cloud. These are only two models, perhaps one more innovative than the other, matching two modes of use of computing resources. While the Ellison model may be “good” for some organisations, the Benioff model is valuable for others, and we can see companies using both in different combinations. Who can be confused about the coexisting modalities of Cloud solutions?

The Benioff-Elison debate tends to reappear when we discuss Security requirements and Identity management projects in the Cloud. Questions arise about the use of Software as a Service or application platform (SaaS and Infrastructure). Which is more secure and which is more efficient?

The conventional IT approach tends to see the Cloud as another new technology and ignore the fact that neither the application nor the platform should be chosen in and by themselves. It is high time that IT professions abandon techno-centric criteria, especially because new technology is not always good. Technology adoption in the usual manner will be especially counterproductive if we do not start from a clear understanding of the role of the users of technology. The needs of these users are the engine of the Internet and the Cloud expansion period. What technologies we use to serve those needs comes second.

To do this we have to study the “access route matrix,” i.e. the combination of user types, device types, credentials, assurance levels, locations and application types that are or will be in play. From the access route matrix we can gather the type of Cloud that will be necessary: Private, Hybrid or Public, and the many combinations between these modalities.

We need to accept the Cloud for what it is: a diverse environment with a multitude of offerings. This environment will not become less complex in the future, but larger and more complex. It is counterproductive to assume that a particular marketing strategy represents the “true cloud” versus all the rest, or that some clever combination of infrastructure and software will rule over all the others. That thinking is anchored in the past, when IT Departments were given the responsibility to “choose” one technology over another and having “one provider” for all needs seemed to be a good idea.

The Cloud transition changes this because in the same way there is no single type of user (e.g. the “enterprise user”); there is also no single “optimal” type of application or infrastructure/platform. It is also the case that different applications can be ideal even if they run on different platforms. Isn’t it the beauty of the Cloud that market forces will decide adoption, technology mix and mobility? Why should a software capability be linked forever to a specific platform or infrastructure?

From a technical point of view it is logical to expect that a particular offering will have enough efficiency, virtualisation, security, redundancy and all the other desirable capabilities, but if you do not face the new landscape of users, partners, third parties, trusted and not-trusted environments at a global scale, how “economic” will your Cloud be?

This is relevant for Identity management solutions, considering that Identity data is not concentrated around any particular point of the network-of-networks that is the Cloud. Identity data performance becomes more critical than old-style security focused on multiple layers of protection around the applications. How you manage identity data contributes more to security than how deep you bury your application. So if the data is not concentrated in any one point and if the enterprise does not own most of the data anymore, where are we going to build our new Chinese wall?

The conventional IT department perspective thinks of the Cloud as an extension of the enterprise realm, and some platform sellers contribute to this mirage by “extending” proprietary platforms as Cloud platforms. This is entirely justified as business strategy from their point of view. During the Cloud transition period, companies and cloud consumers in general will have various combinations of traditional enterprise, private and public Cloud adoption levels, but we must look beyond this towards a period “after the Cloud,” i.e. a period when the Cloud has stopped being a novelty, a marketing term or a “challenge.” An era when the Cloud will be our normal space of action, and there will be no more reason for “false” or “true” doctrines.

Breaking the Ceiling for Cloud Adoption

When discussing the Cloud Transition, we find persistent doubts and demands for increased assurances for data protection, cross-border operations, data ownership and processing, out-sourced operations and service provisioning. As covered in previous chapters, all these aspects can and should be covered in our Security strategy, but the techno-centric views pass over the real limits to Cloud computing, if only Risk issues are important, and, more precisely, only Risk for the enterprise and enterprise “assets.” Risk for the citizen, consumer and employee are addressed, but only as far as they form “informational assets” (which is not always the case), and only to respond to legal duties (data protection and privacy).

This fails to see the real ceiling, for Cloud adoption is not enterprise trust but individual trust, individual (citizen and consumer) confidence in electronic commerce and exchanges. Roughly speaking, “half” of Cloud adoption depends on organisation adopting hosted services to do their business and reduce their IT footprint and costs, but the other “half” (in fact a bigger part of the picture) depends on the users and consumers buying and transacting through the Internet in greater numbers. As Mike

Neuenschwander¹³ suggested some years ago, the “ceiling” for mass adoption lies in lack of user-centric and privacy-centric identity solutions in the hands of the individual and the citizen, and not on the side of the enterprise. In fact, organisations persist in managing users through administrative, centralised, and over-engineered and in reality insecure technologies and only do not have more users because this would be absurdly complex.

This is, though, a still open challenge around developing a socio-economic approach (with a hint of technology only) that will shift our understanding of the Cloud and electronic commerce in general to new protocols and new possibilities. Neuenschwander calls for a “trust protocol” based on social structures, to override the Cloud adoption ceiling.¹⁴

I want to close this chapter by describing how I think this conundrum will be resolved. While I agree with M. Neuenschwander in saying the Cloud needs a “trust protocol” and a “user-centric approach” I am convinced that this is not achievable through a new (or old) “identity platform.” Neuenschwander himself has made suggestive contributions to this matter with his idea of the private “persona” and the “trust protocol,” but this work does not logically lead only or even primarily to a technology or a technological solution that would support these social changes. Above all we need an intellectual revolution bringing us away from the belief that new technologies are necessary for progress. Instead, progress is needed first for new technologies to appear. We need to get the causal chain right. Either the new trust modalities, strategies and plans exist first at least in the mind of the public and organisational leaders, or no technology will ever support user-centric trust.

In fact, I believe that technologies for this change exist and have been available for over a decade. Is there something that Identity experts cannot do with our old and proven Internet protocols? It is not technology that is missing, and we are losing time by attaching our hopes to partial solutions and a multitude of “social media” which do not represent the general interest but just clever business plans.

The trusted protocol and the user-centric solutions will not appear as great ideas once we crack the Identity code from a different angle, that of membership. As the reader is aware by now, the Selection perspective –the one that represents more centrally the vision of Identity management—calls for an idea of identity as “membership,” based on “Trust allocation.” In this sense, a trust protocol is not a technology, but a series of concerted actions to effectively transfer risk and allocate classes of people into multiple assurance levels. So a trust protocol is a process to define, allocate, enforce and verify trust, and not only a mechanism to “score” trust in the Cloud or to enforce some set of rules. Those mechanisms will certainly be necessary, but first a radical evolution of the idea of trust and risk sharing needs to take place, repositioning the disciplines of Security. I hope that in closing this book, I have given good arguments in favour of this transformation.

As we transition to the Cloud, the world *after* the Cloud will light up our steps.

¹ David Chadwick's website: <http://www.cs.kent.ac.uk/people/staff/dwc8/>

² Security practitioners continue to quote the NIST Risk Management Guide for Information Technology Systems, but this publication does not use the concept of "Annualize Loss Expectancy (ALE) anymore! See: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

³ Return on Information Security Investment, see: Adrian Mizzi, "Return on Information Security Investment," 2005, http://www.infosecwriters.com/text_resources/pdf/ROISI.pdf

⁴ See: Jan Willemson, "On the Gordon&Loeb Model for Information Security Investment," WEIS, 2006, <http://weis2006.econinfosec.org/docs/12.pdf>

⁵ The ISC² CISSP body of knowledge manual details: "Risk management minimizes loss to information assets through identification, measurement, and control, and minimizes loss due to events. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost-benefit analysis, management decision, safe-guard implementation, and on-going effectiveness review. Risk management provides the mechanism to the organization to ensure that executive management knows current risks, and decisions are made to accept the risks or implement safeguards to minimize the risks and accept the lower residual risks." CISSP Guide, Auerbach Publications, 2007

⁶ An extraordinary explanation of these terms can be found in the work of the American mathematician Brian Rotman, especially in his book "Mathematics as a Sign," Stanford University Press, 2000.

⁷ Ian Hacking, "The Emergence of Probability," 2006

⁸ N. Carr, "IT Doesn't Matter," Harvard Business Review, May 2004. While Carr still follows a techno-centric model, where technologies are causes and social change is a consequence, he clearly recognises the inevitable fate of the Corporate IT Department.

⁹ Why was user management always sub-optimal? Simple: this type of data was never an asset. Service orientated architecture was never applied to identity data flows because the IT department was always catching up with "the business" project pipeline. There never was time for planning. The IT practitioners know about this sad reality but most do not speak about it. Why was it an illusion that one day architectural patterns would be adopted in the unglamorous world of user administration at least in the same degree as they exist in application development? Why was Access Management - adopted by ITIL as a "process" in 2007—is considered only as part of Service Design but not of Service Operations? The questions are innumerable, but all point back to a refusal to see the fundamental role of the user in Information Technologies.

¹⁰ Marco Casassa Mont, "Economics of Identity and Access Management: providing decision support for investments," Hewlett Packard Laboratories, 2009

See also: "Reducing the costs of IT security Management" CA Technologies (2006)

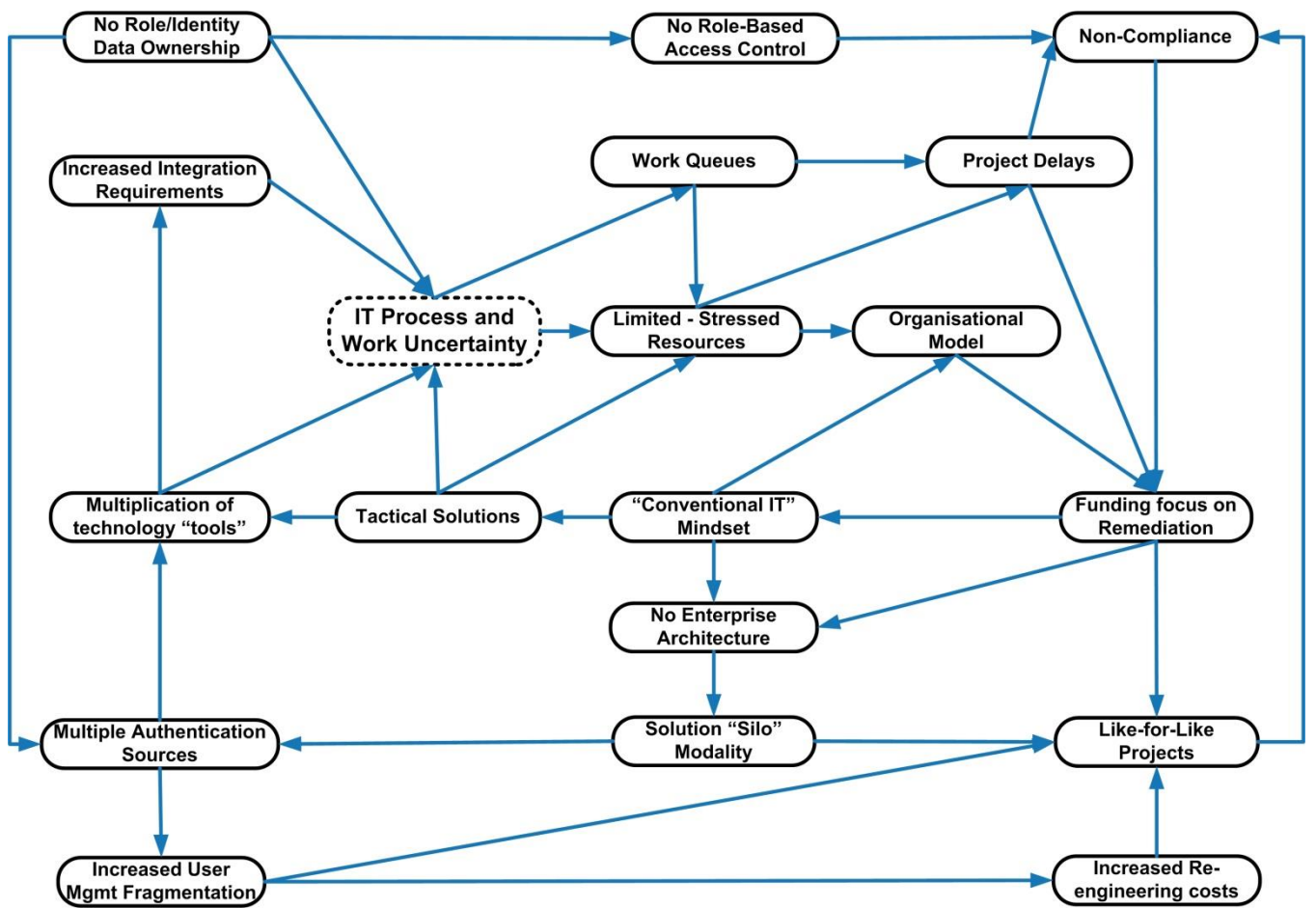
¹¹ <http://www.forbes.com/sites/sap/2011/09/06/larry-ellison-and-marc-benioff-just-cant-agree-what-is-the-cloud/>

¹² <http://www.computerworlduk.com/news/it-business/3308935/larry-ellison-trashes-salesforce-at-oracle-openworld/> and <http://www.informationweek.com/cloud-computing/software/benioff-vs-ellison-this-round-goes-to-sa/228300205>

¹³ M. Neuenschwander, "Thinking outside the domain – The emergence of user centric identity and the trend toward pro-social management systems," 2006, and "Scaling identity to internet proportions," Oracle IDM, April 2012

¹⁴ M. Neuenschwander, "America On The Couch: Analysis Of An Adolescent Society," February 2009. In his blog, Neuenschwander writes: "The Internet enables us to form diverse communities rapidly, introduce environmental variables, monitor behaviours, and investigate community outcomes. Through this kind of research, it may be possible to develop a kind of "trust protocol" that is applicable to a wide range of interactions from financial transactions to social networking. By understanding elements of trust, we may be able to construct a new kind of capitalism, one that avoids the faults and tragedies of youth."

<http://hybridvigor.org/2009/02/27/america-on-the-couch-analysis-of-an-adolescent-society/>



An improved version of the diagram published in "Negative Feedback Chain in Solution Definition and Execution," 2008 see:
<http://carlos-trigoso.com/public/logical-patterns/>

Selected Bibliography

Anderson, R. and T. Moore "The Economics Of Information Security" October 27, 2006

Apelkrans, Mats and Åbom, Carita "Information logistics in a process view," Proceedings to Hawaiian International conference on business, 2002

Arnold, J. "Security Services Model - Security Architecture For The Modern Enterprise," Information Security Bulletin. April, 2006

Ashby, W. R, "An Introduction to Cybernetics," London: Chapman & Hall Ltd. , 1956

Aurobindo, Sri "Letters on Yoga," Collected Works of Sri Aurobindo, 1972

Backhouse, J. and Dhillon, G. "Structures of responsibility and security of information systems," European Journal of Information Systems, 1996

Barwise, J. and Seligman, J "Information Flow – The Logic of Distributed Systems," 1997

Baskerville, R. and Dhillon, G. "Information Systems Security Strategy: A Process View," 2008

Bell, D.E. and LaPadula, L. "Secure Computer Systems: Mathematical Foundations," 1973

Biba, K.J. "Integrity Considerations for Secure Computer Systems," 1977

Blanché, Robert "Structures intellectuelles - Essai sur l'organisation systématique des concepts," ed. J. Vrin, 1966

Burrell, G. and G. Morgan, "Sociological Paradigms Organizational Analysis," Heinemann Press, London, 1979

Cabrera, D. "Systems Thinking: Four Universal Patterns of Thinking," Ithaca, NY: Cornell University, 2006

Canterbury, Anselm of "Complete Philosophical and Theological Treatises of Anselm of Canterbury," translated by Jasper Hopkins and Herbert Richardson, The Arthur J. Banning Press, Minneapolis

Carr, Nicholas "Does IT Matter? Information Technology and the Corrosion of Competitive Advantage," Harvard School Press, 2004

Carr, Nicholas. "IT doesn't matter," Harvard Business Review, May 2003

Casassa Mont, Marco "Economics of Identity and Access Management: providing decision support for investments," Hewlett Packard Laboratories, 2009

Chapman, William, Rozenblit, Jerzy and Bahill, Terry "System design is an NP-complete problem," 2001

Churchman, C. W. "The Systems Approach," 1968

Clark, D. and Wilson, D. "A Comparison of Commercial and Military Computer Security Policies," 1987

Clemons, E. "Strategic necessities," ComputerWorld, 1988

Cobb, Martin "Unfinished Voyages: a follow-up to the CHAOS Report," 1996

Conant, R. C. and Ashby, R. "Every good regulator of a system must be a model of that system," International Journal of Systems Science, 1970

Deiters, W. "The information logistics approach toward a user demand-driven information supply," in Cross Media Service Delivery, 2003

Dhillon, G. A. "Interpreting the Management of Information Systems Security," University of London, 1995

Ellis, K. "The Impact of Business Requirements on the Success of Technology Projects," IAG report, 2008

Ellsberg, D. "Risk, Ambiguity and the Savage Axioms," Quarterly Journal Of Economics, 1961

Evans, Paul "Information Security as a Business Process," IT Network Solutions, 2004

Eveleens, L. and Verhoef, C. "The Rise and Fall of the Chaos Report Figures," IEEE Software magazine, 2010

Fiske, Alan. P., and Haslam, N. "The Four Basic Social Bonds: Structures For Coordinating Interaction," in Interpersonal Cognition, 2005

Forrester, Jay W. "Principles of Systems," MIT Press, 1968

Galbraith, Jay "Organizational Design: An Information Processing View," 1974

Gigerenzer, G. and Goldstein, D. "Reasoning The Fast and Frugal Way: Models Of Bounded Rationality," Psychological Review, 1966

Goguen, Joseph and Meseguer, J. "Security Policies and Security Models," 1982

Gottschalk, Walter Helbig "Theory of Quaternality," 1953

Hacking, Ian "The Emergence of Probability," 2006

Hegel, G.W.F "Wissenschaft der Logik," 1812

Heidegger, Martin "The Thing," 1950

Hirschheim, Rudy and Heinz K. Klein, "Four Paradigms Of Information System Development," Communications Of The ACM, October 1989

Hohfeld, Wesley Newcomb "Fundamental Legal Conceptions," 1978

Jung, Richard "A Quaternion of Metaphors for the Hermeneutics of Life," 1985

Kahneman, D. and Tversky, A. "Prospect Theory: An Analysis Of Decision Under Risk," Econometrica, 1979

Kant, I. "Critique of Pure Reason," 1781

Kelly, George A. "The Psychology of Personal Constructs," 1955

Kreps, D. M. "A Course In Microeconomic Theory," 1990

Krigsman, Michael <http://www.zdnet.com/blog/projectfailures/research-75-percent-believe-it-projects-are-doomed/13016>

Kuhn, T. S., "The Structure of Scientific Revolutions," The University of Chicago Press, 1970

Lacan, Jacques, "Encore," Séminaire Livre XX, Paris 1975

Landoll, D. J., and J. Williams, R. "An Enterprise Assurance Framework," Arca Systems, Inc. <http://www.sse-Cmm.org/docs/WetIce.pdf>

Lofting, Chris "The Neurocognitive Roots of Logic," 2003

Luhmann, Niklas "Soziologie des Risikos," de Gruyter, 1991

Maruyama, Magoroh "Individual Types: Subcultural Or Transcultural," The General Psychologist, 2001

Maturana, Humberto and Varela, Francisco "Autopoiesis and Cognition: the Realization of the Living," 1973

McFadzean, Elspeth, Ezingear, Jean-Noël and Birchall, David, "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," Henley Management College, 2004

McLean, J. "Security Models and Information Flow," 2003

McWhinney, W. "Paths of Change: Strategic Choices for Organizations and Society," 1992

Mitchell Donald, Coles, Carol and Metz, Robert "The 2,000 Percent Solution: Free Your Organization from Stalled Thinking to Achieve Exponential Success," 1999

Mohanty, Ashok "Mathematical model for expediting the execution of projects," 2011

Moretti, Alessio "The Geometry of Logical Opposition," 2009

Morgan, Gareth and Burrell, Gibson, "Sociological Paradigms and Organisational Analysis," 1979

Moroney, Stephen K. "The Noetic Effects of Sin," 2000

Neuenschwander, M. "Thinking outside the domain – The emergence of user centric identity and the trend toward pro-social management systems," 2006

Palmquist, Steven "The Combination Of Analysis and Synthesis In Numerical Symbolism," Kant on the Web and The Geometry of Logic <http://staffweb.hkbu.edu.hk/ppp/>

Parker, Donn B. "Making the Case For Replacing Risk Based Security," The ISSA Journal, 2006

Peil, J. "Einige Bemerkungen zu Problemen der Anwendung des Informationsbegriffs in der Biologie," 1971

Peirce, C. S. "Collected Papers," Harvard University Press, 1948

Pepper, Stephen C. "World Hypotheses – A Study in Evidence," 1942

Petrauskas, Vaidotas "The Use of Information Flow Analysis For Building An Effective Organization," Information Technology and Control, 2006

Phillips, Robert L. "The Management Information Value Chain," Perspectives, Issue 3

Piaget, Jean "Traité de logique. Essai de logistique opératoire," 1972

Raywood, Dan, "Jericho Forum: Identity and access management need to be separated in the business," 2011

Ropohl, Günter "Allgemeine Technologie : eine Systemtheorie der Technik," Universität Karlsruhe, 2009

Roszak, Theodore "The Cult of Information," Pantheon, 1986

Rotman, Brian "Mathematics as a Sign," Stanford University Press, 2000.

Savage, Leonard J. "The Foundations Of Statistics," Wiley, 1954

Seccombe, Adrian "Identity the New Perimeter," Surrey University, 2010

Shannon, C. E. and Weaver, W. "The Mathematical Theory of Communication," University of Illinois Press, 1949

Sholle, D. "What is Information? The Flow of Bits and the Control of Chaos," <http://web.mit.edu/comm-forum/papers/sholle.html>

Simon, Herbert. A. "A Behavioral Model Of Rational Choice," Quarterly Journal Of Economics, 1955

Soo Hoo, Kevin "How Much Is Enough? A Risk-Management Approach to Computer Security," 2000

Stiglitz, Joseph E. "The Contributions Of The Economics Of Information To Twentieth Century Economics," Quarterly Journal Of Economics, November 2000

Strassman, Paul A. "The Business Value of Computers," Information Economics Press, 1990

Sutherland, D. "A Model of Information," 1986

Thatcher, Matt E. and Pingry, David E. "Modeling the IT Value Paradox," Communications of the ACM, August 2007

Uckelman, Sara L. "Anselm's logic of agency," Institute for Logic, Language, and Computation, 2009

Wallace, A.F.C. "On Being Just Complicated Enough," 1961

Walton, Douglas "St. Anselm and The Logical Syntax of Agency," Franciscan Studies, 1976

Wang, R. Y., Kon, H. B. and Madnick, S. E., "Data Quality Requirements Analysis and Modeling," 1992

Weizsäcker, E. "Offene Systeme I – Beiträge zur Zeitstruktur von Information, Entropie und Evolution," 1974

White, Hayden "Metahistory: The Historical Imagination in Nineteenth-Century Europe," The Johns Hopkins University Press, 1973

Wiener, Norbert "Cybernetics, or control and communication in animal and machine," MIT Press 1961

Wierenga, Hans, "Why the Information Security Consultancy Industry Needs a Major Overhaul," 2010
<http://www.soamag.com/142/0810-1.php>

Williams, J. R., and G. F. Jelen "A Framework for Reasoning About Assurance," Arca Systems, April 23, 1998

Zhang, Kan "A theory for Systems Security," Cambridge University, 1997

